

**To:** CampusGuard([kstaples@campusguard.com](mailto:kstaples@campusguard.com))  
**Subject:** U.S. Trademark Application Serial No. 97777513 - REDLENS INFOSEC  
**Sent:** November 01, 2023 07:41:30 PM EDT  
**Sent As:** [tmng.notices@uspto.gov](mailto:tmng.notices@uspto.gov)

---

**Attachments**

[7165721](#)  
[5696063](#)  
[screenshot-encyclopedia2-thefreedictionary-com-infosec-16988691083961](#)  
[screenshot-encyclopedia2-thefreedictionary-com-information-security-16988691820401](#)  
[screenshot-en-wikipedia-org-wiki-Information\\_security-16988692644361](#)

**United States Patent and Trademark Office (USPTO)**  
**Office Action (Official Letter) About Applicant's Trademark Application**

**U.S. Application Serial No.** 97777513

**Mark:** REDLENS INFOSEC

**Correspondence Address:**  
CAMPUSGUARD  
121 SOUTH 13TH STREET  
LINCOLN NE 68508  
UNITED STATES

**Applicant:** CampusGuard

**Reference/Docket No.** N/A

**Correspondence Email Address:** [kstaples@campusguard.com](mailto:kstaples@campusguard.com)

**NONFINAL OFFICE ACTION**

**Response deadline.** File a response to this nonfinal Office action within three months of the “Issue date” below to avoid [abandonment](#) of the application. Review the Office action and respond using one of the links to the appropriate electronic forms in the “How to respond” section below.

**Request an extension.** For a fee, applicant may [request one three-month extension](#) of the response deadline prior to filing a response. The request must be filed within three months of the “Issue date” below. If the extension request is granted, the USPTO must receive applicant's response to this letter within six months of the “Issue date” to avoid abandonment of the application.

**Issue date:** November 1, 2023

**How to respond.** File a [response form to this nonfinal Office action](#) or file a [request form for an extension of time to file a response](#).

\* \* \* \* \*

The referenced application has been reviewed by the assigned trademark examining attorney. Applicant must respond timely and completely to the issue(s) below. 15 U.S.C. §1062(b); 37 C.F.R. §§2.62(a), 2.65(a); TMEP §§711, 718.03.

### **SEARCH OF USPTO DATABASE OF MARKS (Advisory)**

The trademark examining attorney has searched the USPTO database of registered and pending marks and has found no conflicting marks that would bar registration under Trademark Act Section 2(d). 15 U.S.C. §1052(d); TMEP §704.02.

Applicant must respond to the requirement(s) set forth below.

### **DISCLAIMER REQUIRED**

Applicant must disclaim the wording “INFOSEC ” because it is merely descriptive of an ingredient, quality, characteristic, function, feature, purpose, or use of applicant’s goods and/or services. *See* 15 U.S.C. §§1052(e)(1), 1056(a); *DuoProSS Meditech Corp. v. Inviro Med. Devices, Ltd.*, 695 F.3d 1247, 1251, 103 USPQ2d 1753, 1755 (Fed. Cir. 2012); TMEP §§1213, 1213.03(a).

The term INFOSEC is short for " Information security" and "is the practice of protecting information by mitigating information risks." See attached definitions. Here, the wording describes the services which are in the field of information security or for information security. The Office has required the disclaimer of other marks comprising of INFOSEC for similar goods or services. See attached U.S. Registrations.

Applicant may respond to this issue by submitting a disclaimer in the following format:

**No claim is made to the exclusive right to use “INFOSEC” apart from the mark as shown.**

For an overview of disclaimers and instructions on how to provide one using the Trademark Electronic Application System (TEAS), see the [Disclaimer webpage](#).

A “disclaimer” is a statement in the application record that an applicant does not claim exclusive rights to an unregistrable component of the mark. *See Schwarzkopf v. John H. Breck, Inc.*, 340 F.2d 978, 979-80, 144 USPQ 433, 433 (C.C.P.A. 1965); TMEP §1213. A disclaimer does not physically remove the

disclaimed matter from the mark or otherwise affect the appearance of the mark. *See Schwarzkopf v. John H. Breck, Inc.*, 340 F.2d at 979, 144 USPQ2d at 433; TMEP §1213.

If applicant does not provide the required disclaimer, the USPTO may refuse to register the entire mark. *See In re Stereotaxis Inc.*, 429 F.3d 1039, 1041, 77 USPQ2d 1087, 1089 (Fed. Cir. 2005); TMEP §1213.01(b).

## **IDENTIFICATION AND CLASSIFICATION**

Applicant has provided the following identification and classification of goods and/ or services in its application:

International Class 042: We provide cybersecurity and compliance services such as pen testing, PCI compliance, security awareness training, IT security consulting service, etc

The identification of services is unacceptable as indefinite because it is too broad and could include services in other international classes and must be clarified. *See* 37 C.F.R. §2.32(a)(6); TMEP §§1402.01, 1402.03. Applicant must amend the identification to specify the common commercial or generic name of the services. *See* TMEP §1402.01. If the services have no common commercial or generic name, applicant must describe or explain the nature of the services using clear and succinct language. *See id.*

The wording “etc” in the identification of services is indefinite and must be clarified because it fails to identify specific services. *See* TMEP §1402.03(a). Therefore, applicant must delete this indefinite wording from the identification and specify the common commercial or generic name for these services.

In an identification, an applicant must use the common commercial or generic name for the services, be specific and all-inclusive, and avoid using indefinite words or phrases. TMEP §§1402.01, 1402.03(a). Further, applicant may amend the identification to list only those items that are within the scope of the services set forth in the initial application or as acceptably amended. *See* 37 C.F.R. §2.71(a); TMEP §§1402.06 *et seq.*, 1402.07. Scope is generally determined by the ordinary meaning of the wording in the identification. TMEP §1402.07(a).

The Trademark Act requires that a trademark or service mark application must include a “**specification** of ... the goods [or services]” in connection with which the mark is being used or will be used. 15 U.S.C. §1051(a)(2) (emphasis added), (b)(2) (emphasis added); *see* 15 U.S.C. §1053. Specifically, a complete application must include a “list of the **particular** goods or services on or in connection with which the applicant uses or intends to use the mark.” 37 C.F.R. §2.32(a)(6) (emphasis added). This requirement for a specification of the particular goods and/or services applies to applications filed under all statutory bases. *See* 15 U.S.C. §§1051(a)(2), 1051(b)(2), 1053, 1126(d)-(e), 1141f; 37 C.F.R. §2.32(a)(6); TMEP §§1402.01, 1402.01(b)-(c).

The USPTO has the discretion to determine the degree of particularity needed to clearly identify goods and/or services covered by a mark. *In re SICPA Holding*, 2021 USPQ2d 613, at \*4 (TTAB 2021) (quoting *In re Omega SA*, 494 F.3d 1362, 1365, 83 USPQ2d 1541, 1543-44 (Fed. Cir. 2007)). Accordingly, the USPTO requires the description of goods and/or services in a U.S. application to be

specific, definite, clear, accurate, and concise. *In re tapio GmbH*, 2020 USPQ2d 11387, at \*6 (TTAB 2020) (quoting *In re Cordua Rests., Inc.*, 823 F.3d 594, 605, 118 USPQ2d 1632, 1639 (Fed. Cir. 2016)); TMEP §1402.01.

Applicant may adopt the following identification, if accurate:

- Training services in the field of cybersecurity awareness (INT. CLASS 41)
- Data security consultancy; IT cybersecurity consulting service; Computer security consultancy to identify security weaknesses and vulnerabilities across enterprises and to assist in remediating any security deficiencies through penetration testing, payment card industry (PCI) compliance, vulnerability assessments, password auditing, and cyberattack simulation (INT. CLASS 42)

**Amendment of Classification Advisory:** If applicant adopts the suggested amendment of the identification of goods and/or services, then applicant must amend the classification to **add** International Class(es) 41. *See* 37 C.F.R. §§2.32(a)(7), 2.85; TMEP §§805, 1401.

**Scope Advisory:** Applicant's goods and/or services may be clarified or limited, but may not be expanded beyond those originally itemized in the application or as acceptably amended. *See* 37 C.F.R. §2.71(a); TMEP §1402.06. Applicant may clarify or limit the identification by inserting qualifying language or deleting items to result in a more specific identification; however, applicant may not substitute different goods and/or services or add goods and/or services not found or encompassed by those in the original application or as acceptably amended. *See* TMEP §1402.06(a)-(b). The scope of the goods and/or services sets the outer limit for any changes to the identification and is generally determined by the ordinary meaning of the wording in the identification. TMEP §§1402.06(b), 1402.07(a)-(b). Any acceptable changes to the goods and/or services will further limit scope, and once goods and/or services are deleted, they are not permitted to be reinserted. TMEP §1402.07(e).

For assistance with identifying and classifying goods and services in trademark applications, please see the USPTO's online searchable [\*U.S. Acceptable Identification of Goods and Services Manual\*](#). *See* TMEP §1402.04.

## **MULTIPLE – CLASS APPLICATION REQUIREMENTS**

The application identifies goods and/or services in more than one international class; therefore, applicant must satisfy all the requirements below for each international class based on Trademark Act Section 1(b) :

- (1) **List the goods and/or services by their international class number** in consecutive numerical order, starting with the lowest numbered class.

(2) **Submit a filing fee for each international class** not covered by the fee(s) already paid (view the [USPTO's current fee schedule](#)). The application identifies goods and/or services that are classified in at least 2 classes; however, applicant submitted a fee(s) sufficient for only 1 class(es). Applicant must either submit the filing fees for the classes not covered by the submitted fees or restrict the application to the number of classes covered by the fees already paid.

*See* 37 C.F.R. §2.86(a); TMEP §§1403.01, 1403.02(c).

For an overview of the requirements for multiple-class application and how to satisfy the requirements online using the Trademark Electronic Application System (TEAS) form, see the [Multiple-class Application webpage](#).

## **PERSONS WHO CAN SIGN RESPONSES – Advisory**

**Persons who can properly sign responses.** If an applicant is not represented by a U.S.-licensed attorney qualified under 37 C.F.R. §11.14, the response must be signed by the individual applicant or someone with legal authority to bind a juristic applicant (e.g., a corporate officer or general partner). *See* 37 C.F.R. §2.193(e)(2)(ii); TMEP §611.03(b). In the case of joint applicants, all must sign. 37 C.F.R. §2.193(e)(2)(ii); TMEP §611.06(a).

TMEP §611.06(g) provides the following regarding signature by Limited Liability Company:  
A limited liability company ("LLC") has attributes of both a corporation and a partnership. *See* TMEP §803.03(h). Generally, a signatory identified as "manager," "member," "principal," or "owner" may be presumed to have the authority to sign on behalf of a domestic or foreign limited liability company. In addition, anyone with a corporate-officer-type title, such as "President" or "Chief Executive Officer," may sign.

If an applicant is represented by a U.S.-licensed attorney qualified under 37 C.F.R. §11.14, the attorney must sign the response. 37 C.F.R. §2.193(e)(2)(i); TMEP §611.03(b). The only attorneys who may sign responses are (1) attorneys in good standing with a bar of the highest court of any U.S. state or territory, or (2) Canadian trademark attorneys or agents [reciprocally recognized](#) by the USPTO's Office of Enrollment and Discipline (OED) to represent applicants located in Canada and who are working under a qualified U.S.-licensed attorney. *See* 37 C.F.R. §§2.17(a), 11.14(a), (c), (e); TMEP §602. Foreign attorneys, other than recognized Canadian trademark attorneys or agents, do not have authority to sign responses. *See* 37 C.F.R. §§2.17(e), 11.14(c)(1), (e); TMEP §602.03-.03(a).

In all cases, the signer's first and last name and title or position must be specified immediately below or adjacent to the signature. 37 C.F.R. §2.193(d); TMEP §611.01(b).

## **CLOSING**

Because of the legal technicalities and strict deadlines of the trademark application process, applicant is encouraged to hire a private attorney who specializes in trademark matters to assist in this process. See [Hiring a U.S.-licensed trademark attorney](#) for more information. USPTO staff cannot provide legal advice or statements about an applicant's legal rights. TMEP §§705.02, 709.06. The assigned trademark examining attorney can provide only limited assistance explaining the content of an Office action and the application process. For general questions and status inquiries, please contact the Trademark Assistance Center at (800) 786-9199. <https://www.uspto.gov/learning-and-resources/support-centers/trademark-assistance-center>

Informal communications may not be used to request advisory opinions as to the likelihood of overcoming a substantive refusal. The examining attorney should advise the applicant to file a formal response for consideration of arguments regarding any substantive refusal. TMEP §709.05. For a legal opinion about any trademark matter, a party must consult a private trademark attorney. TMEP §1805.

**Response guidelines.** For this application to proceed, applicant must explicitly address each refusal and/or requirement in this Office action. For a refusal, applicant may provide written arguments and evidence against the refusal, and may have other response options if specified above. For a requirement, applicant should set forth the changes or statements. Please see “[Responding to Office Actions](#)” and the informational [video “Response to Office Action”](#) for more information and tips on responding.

NOTE: If applicant requires assistance navigating the online response form, applicant should contact the Trademark Assistance Center at (800) 786-9199.

/Benji Paradewelai/  
Trademark Examining Attorney  
USPTO, Law Office 101  
(571) 272-1658  
[Benji.Paradewelai@USPTO.GOV](mailto:Benji.Paradewelai@USPTO.GOV)

## **RESPONSE GUIDANCE**

- **Missing the deadline for responding to this letter will cause the application to [abandon](#).** A response or extension request must be received by the USPTO before 11:59 p.m. **Eastern Time** of the last day of the response deadline. Trademark Electronic Application System (TEAS) [system availability](#) could affect an applicant's ability to timely respond. For help resolving technical issues with TEAS, email [TEAS@uspto.gov](mailto:TEAS@uspto.gov).

- **Responses signed by an unauthorized party** are not accepted and can **cause the application to abandon**. If applicant does not have an attorney, the response must be signed by the individual applicant, all joint applicants, or someone with **legal authority to bind a juristic applicant**. If applicant has an attorney, the response must be signed by the attorney.
- If needed, **find contact information for the supervisor** of the office or unit listed in the signature block.

7165721

# Hudson Infosec

<b>Word Mark</b>	HUDSON INFOSEC •
<b>Goods/Services</b>	IC 042 US 101 100 Technology consultation in the field of cyber security including conducting cybersecurity auditing; cloud data migration services and software development related thereto.
<b>Register</b>	PRINCIPAL
<b>Serial Number</b>	97248054
<b>Filing Date</b>	2022-02-01T00:00:00
<b>Original Filing Basis</b>	1b
<b>Current Filing Basis</b>	1a
<b>Publication Date</b>	2022-12-20
<b>Registration Number</b>	7165721
<b>Date Registered</b>	2023-09-12
<b>Owner</b>	(REGISTRANT) Hudson Infosec LLC (LIMITED LIABILITY COMPANY; NEW YORK); 1 Crestwood Blvd, Poughkeepsie, NEW YORK 12603, UNITED STATES
<b>Type of Mark</b>	SERVICE MARK
<b>Mark Drawing Code</b>	(4) STANDARD CHARACTER MARK
<b>Disclaimer</b>	"INFOSEC"
<b>Live Dead Indicator</b>	LIVE
<b>Status</b>	REGISTERED





5696063



**Word Mark**

BERYLLIUM INFOSEC COLLABORATIVE

•

IC 042 US 101 100

**Goods/Services**

Consulting in the field of information technology; Computer security consultancy in the field of scanning and penetration testing of computers and networks to assess information security vulnerability; Computer services, namely, acting as an application service provider in the field of information management to host computer application software for the purpose of securing company or US government sensitive but unclassified information; Computer services, namely, cloud hosting provider services; Computer software consulting; Development of security systems and contingency planning for information systems; Development of customized software for others for use in risk assessment, information security, business analysis, audit and audit planning, and sales management; Information technology consulting services; IT consulting services; Outsource service provider in the field of information technology consulting; Providing a website that features technology that enables the secure exchange of information by users; Software as a service (SAAS) services, namely, hosting software for use by others for use in securely storing, manipulating and transmitting sensitive information.; Technical support services, namely, remote administration and management of in-house and hosted datacenter devices, databases and software applications.

**Register**

PRINCIPAL

**Serial Number**

88032349

**Filing Date**

2018-07-10T00:00:00

**Original Filing Basis**

1a

**Current Filing Basis**

1a

**Publication Date**

2018-12-25

**Registration Number**

5696063

**Date Registered**

2019-03-12

<b>Owner</b>	<ul style="list-style-type: none"> <li>• (REGISTRANT) Beryllium, LLC (LIMITED LIABILITY COMPANY; MINNESOTA); Suite 210, 715 Florida Ave S, Minneapolis, MINNESOTA 55426, UNITED STATES</li> <li>• (LAST LISTED OWNER) BERYLLIUM INFOSEC, INC. (CORPORATION; DELAWARE); 715 FLORIDA AVENUE S, SUITE 210, MINNEAPOLIS, MINNESOTA 55426, UNITED STATES</li> </ul>
<b>Type of Mark</b>	SERVICE MARK
<b>Mark Drawing Code</b>	(3) DESIGN PLUS WORDS, LETTERS, AND/OR NUMBERS
<b>Design Code</b>	260113, 260121, 261503
<b>Description of Mark</b>	<ul style="list-style-type: none"> <li>• The color(s) green, and dark blue is/are claimed as a feature of the mark.</li> <li>• The mark consists of a green hexagonal outline surrounding the dark blue capital letters, "BERYLLIUM". The base of the hexagonal outline is broken by two dark blue nodes interrupted by the words, "InfoSec Collaborative" in dark blue letters.</li> </ul>
<b>Disclaimer</b>	"INFOSEC" AND "COLLABORATIVE"
<b>Live Dead Indicator</b>	LIVE
<b>Status</b>	REGISTERED
<b>Attorney of Record</b>	Craig Carpenter

**Print:** November 1, 2023 11:48 AM

THE FREE DICTIONARY

BY FARLEY

13,672,062,371 visits served

infosec

Word / ArticleStarts withEnds withText

Register

Log in

Sign up with one click

Share 25K

DictionaryThesaurusMedical DictionaryLegal DictionaryFinancial DictionaryAcronymsIdiomsEncyclopediaWikipedia Encyclopedia

f

t

"CITE"

Instant Grammer Checker

Correct all grammar errors and enhance *your* writing.

Try Now

infosec

Also found in: Dictionary, Acronyms.

infosec

Short for "information security." The term was primarily used in the military (INFOSEC) and migrated to commercial parlance. Also "Infosecurity." See [information security](#).

"CITE"

Copyright © 1981-2023 by The Computer Language Company Inc. All Rights reserved. THIS DEFINITION IS FOR PERSONAL USE ONLY. All other reproduction is strictly prohibited without permission from the publisher.

Want to thank TFD for its existence? Tell a friend about us, add a link to this page, or visit the webmaster's page for free fun content.

Link to this page:

<a href="https://encyclopedia2.thefreedictionary.com/infosec">infosec</a>

f

t

Feedback

Instant Grammar Checker

Correct all grammar errors and enhance your writing.

Try Now

Flashcards & Bookmarks

Please [log in](#) or [register](#) to use Flashcards and Bookmarks. You can also log in with

Instant Grammar Checker

Correct all grammar errors and enhance your writing.

Try Now

Mentioned in

CIA  
NSTISSI  
Triad

References in periodicals archive

This is Cyber Defense Magazine's seventh year of honoring InfoSec innovators.  
*Cyber Defense Magazine Names PC Pitstop, Makers of PC Matic Pro, Market Leader in Malware Detection*

InfoSec can be complex and hard, but is always crucial.  
*Wake up to security threats: Protecting your organization, its reputation and its confidential data is of imperative importance*

Consequently, a major component of infosec is simply getting personnel to follow practices that they should be doing already.  
*RED ALERT: EVOLVING CYBER ATTACKS ARE FORCING BUSINESSES TO STAY VIGILANT*

The latest DOD Internet Services and Internet-based Capabilities Instruction, DOD Instruction 8550.01, states that "DoD employees shall be educated and trained to conduct both organizational and individual communication effectively to deny adversaries the opportunity to take advantage of information that may be inappropriately disseminated." (21) Although most technical threats posed by SNSs can be mitigated through the proper use of security measures already in place in most Air Force networks that is perimeter defenses, firewalls, and so forth, information and operations security hinges

Encyclopedia browser

informed consent  
Informer  
Informix  
Informosome  
Informosomes  
Infotunes  
Infosec  
InfoSeek  
InfoStreet, Inc.  
Infotainer  
infotainment  
infotech  
infoware  
InfoWindow

Full browser

Intosid

InfoScore Consumer Data

Infoscreen Networks Plc

InfoSearch Media, Inc.

Infosec

INFOSEC Assessment - Capability Maturity Model

INFOSEC Assessment Methodology

Infosec Assessment Training and Rating Program

INFOSEC Integration and Oversight Office

InfoSec News

THE FREE DICTIONARY

BY FARLEX

13,672,064,382 visits served

information security

Word / Article

Starts with

Ends with

Text

Register

Log in

Sign up with one click

Share 25k

Dictionary

Thesaurus

Medical Dictionary

Legal Dictionary

Financial Dictionary

Acronyms

Idioms

Encyclopedia

Wikipedia Encyclopedia

f

t

"CITE"

information security

Also found in: Dictionary, Thesaurus, Medical, Legal, Financial, Acronyms, Wikipedia.

information security

The protection of data against unauthorized access. Programs and data can be secured by issuing passwords and digital certificates to authorized users. However, passwords only validate that a correct number has been entered, not that it is the actual person. Digital certificates and biometric techniques (fingerprints, eyes, voice, etc.) provide a more secure method (see authentication). After a user has been authenticated, sensitive data can be encrypted to prevent eavesdropping (see cryptography).

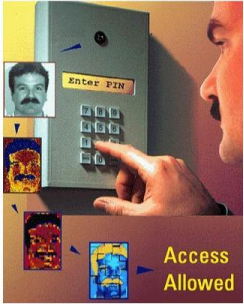
Authorized Users Can Be the Most Dangerous

Although precautions can be taken to authenticate users, it is much more difficult to determine if an authorized employee is doing something malicious. Someone may have valid access to an account for updating, but determining whether phony numbers are being entered requires a great deal more processing. The bottom line is that effective security measures are always a balance between technology and personnel management. See Parkerian hexad, information assurance, security scan, security audit, audit trail, NCSC, ICSA, access control, share-level security, user-level security and social engineering.

Feedback

Flashcards & Bookmarks

Please log in or register to use Flashcards and Bookmarks. You can also log in with



The image shows a person's face being scanned by a facial recognition system. A small inset shows a person's face with a mustache. Below the main image, there are three smaller images showing different faces. The text 'Access Allowed' is displayed in yellow. The interface includes a 'Enter PIN' label and a numeric keypad.

Facial Recognition

Facial recognition is one of the best ways to authenticate a person. This TrueFace system from Miros uses neural network technology to distinguish a face with different appearances, such as with and without glasses and changing hair styles. (Image courtesy of Miros.)

Inc.)

**"CITE"** Copyright © 1981-2023 by The Computer Language Company Inc. All Rights reserved. THIS DEFINITION IS FOR PERSONAL USE ONLY. All other reproduction is strictly prohibited without permission from the publisher.

Want to thank TFD for its existence? Tell a friend about us, add a link to this page, or visit the webmaster's page for free fun content.

Link to this page:

[information security](https://encyclopedia2.thefreedictionary.com/information+security)



Mentioned in

access control

air gapped

audit trail

authenticity

availability

capability

CISA

CISM

cloud computing security

Cloud Security Alliance

computer security

Computer Security Act

confidentiality

CSO

...

References in periodicals archive

Assistant to President - Secretary of Defense Council Kalmukhambet Kassymov at the session said that the **information security** influences economic, social, political aspects and becomes a key element of national security of the country. A special attention was paid to the problem of spreading false information aimed at distabilizing the situation.  
*information security problems discussed in Kazakhstan*

Nator has previously spent a decade at Societe Generale (SocGen) (SOGN PA) (OTC: SCGLY) (GLE FR), including most recently as chief **information security** officer for the Americas region.  
*Bank Leumi USA names chief information security officer*

In January 2018, Camelot received a new cycle of ISO-27001 **information security** management certification, which is inseparable from the Group's ongoing **information security** management system around the standard.  
*Camelot Information System - Camelot comprehensively improves IT service information security management system - 26/4/2019*

On this occasion, Shaikh Khalifa bin Ebrahim Al Khalifa, Chief Executive Officer of Bahrain Bourse, commented: Bahrain Bourse was keen to join the **Information Security** program 'Thiqa' (Trust) as part of its effective approach and

Encyclopedia browser

information resources

information resources management


Full browser

ABC Information Sciences Technology Office

Information Science

Information Retrieval  
Information Retrieval Language  
Information Retrieval System  
Information Science  
► **Information security**  
information selection systems  
information separator  
information service  
information services  
information signs displayed at airports  
information society  
Information Source

ABC Information Scientifique et technique  
ABC Information Screening and Delivery System  
ABC Information Screening and Display Subsystem  
► **Information security**  
ABC Information Security & Network Research Group  
ABC Information Security & Networking Professionals  
ABC Information Security Administration  
ABC Information Security Analysis Program  
ABC Information Security and Assurance

More from 

Mobile  
Apps



Free Tools

For surfers: [Free toolbar & extensions](#) | [Word of the Day](#) | [Word Finder](#) | [Help](#)  
For webmasters: [Free content](#) | [Linking](#) | [Linkup box](#)

[Terms of Use](#) | [Privacy policy](#) | [Feedback](#) | [Advertise with Us](#) | Copyright © 2003-2023 Farlex, Inc

Disclaimer

All content on this website, including dictionary, thesaurus, literature, geography, and other reference data is for informational purposes only. This information should not be considered complete, up to date, and is not intended to be used in place of a visit, consultation, or advice of a legal, medical, or any other professional.



Contents [hide]

(Top)

Definition

>Overview

History

>Basic principles

>Risk management

>Process

Business continuity

Laws and regulations

Culture

Sources of standards

See also

References

>Further reading

External links

## Information security

48 languages

ArticleTask

ReadEditView historyTools

From Wikipedia, the free encyclopedia

(Redirected from InfoSec)

**Information security**, sometimes shortened to **InfoSec**<sup>[1]</sup> is the practice of protecting *information* by mitigating information risks. It is part of information risk management.<sup>[2][3]</sup> It typically involves preventing or reducing the probability of unauthorized or inappropriate access to data or the unlawful use, disclosure, disruption, deletion, *corruption*, modification, inspection, recording, or devaluation of information.<sup>[4]</sup> It also involves actions intended to reduce the adverse impacts of such incidents. Protected information may take any form, e.g., electronic or physical, tangible (e.g., paperwork) or intangible (e.g., knowledge).<sup>[5][6]</sup> Information security's primary focus is the balanced protection of data *confidentiality*, *integrity*, and *availability* (also known as the "CIA" triad) while maintaining a focus on efficient *policy* implementation, all without hampering organization *productivity*.<sup>[7]</sup> This is largely achieved through a structured risk management process that involves:

- Identifying information and related *assets*, plus potential *threats*, *vulnerabilities*, and *impacts*;
- Evaluating the risks;
- Deciding how to address or treat the risks, (i.e., to avoid, mitigate, share, or accept them
- Where risk mitigation is required, selecting or designing appropriate security controls and implementing them
- Monitoring the activities and making adjustments as necessary to address any issues, changes, or improvement opportunities<sup>[8]</sup>

To standardize this discipline, academics and professionals collaborate to offer guidance, policies, and industry standards in passwords, antivirus software, firewalls, encryption software, legal liability, security awareness and training, and so forth.<sup>[9]</sup> This standardization may be further driven by a wide variety of laws and regulations that affect how data is accessed, processed, stored, transferred, and destroyed.<sup>[10]</sup> However, the implementation of any standards and guidance within an entity may have limited effect if a culture of *continual improvement* is not adopted.<sup>[11]</sup>

### Definition [edit]

Various definitions of information security are suggested below, summarized from different sources.

- "Preservation of confidentiality, integrity and availability of information. Note: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved." (ISO/IEC 27000:2018)<sup>[12]</sup>
- "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability." (CNSS, 2010)<sup>[13]</sup>
- "Ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability)." (ISACA, 2000)<sup>[14]</sup>
- "Information Security is the process of protecting the intellectual property of an organisation." (Pipkin, 2000)<sup>[15]</sup>
- "...information security is a risk management discipline, whose job is to manage the cost of information risk to the business." (McDemott and Geer, 2001)<sup>[17]</sup>
- "A well-informed sense of assurance that information risks and controls are in balance." (Anderson, J., 2003)<sup>[18]</sup>
- "Information security is the protection of information and minimizes the risk of exposing information to unauthorized parties." (Venier and Eloff, 2003)<sup>[19]</sup>
- "Information Security is a multidisciplinary area of study and professional activity which is concerned with the development and implementation of security mechanisms of all available types (technical, organizational, human-oriented and legal) in order to keep information in all its locations (within and outside the organization's perimeter) and, consequently, information systems, where information is created, processed, stored, transmitted and destroyed, free from threats.<sup>[20]</sup> Threats to information and information systems may be categorized and a corresponding security goal may be defined for each category of threats.<sup>[21]</sup> A set of security goals, identified as a result of a threat analysis, should be revised periodically to ensure its adequacy and conformance with the evolving environment.<sup>[22]</sup> The currently relevant set of security goals may include: *confidentiality*, *integrity*, *availability*, *privacy*, *authenticity* & *trustworthiness*, *non-repudiation*, *accountability* and *audability*." (Cherdantseva and Hilton, 2013)<sup>[23]</sup>
- Information and information resource security using telecommunication system or devices means protecting information, information systems or books from unauthorized access, damage, theft, or destruction (Kurose and Ross, 2010).<sup>[24]</sup>



At the core of information security is information assurance, the act of maintaining the confidentiality, integrity, and availability (CIA) of information, ensuring that information is not compromised in any way when critical issues arise.<sup>[26]</sup> These issues include but are not limited to natural disasters, computer/server malfunction, and physical theft. While paper-based business operations are still prevalent, requiring their own set of information security practices, enterprise digital initiatives are increasingly being emphasized.<sup>[26][27]</sup> With information assurance now broadly being dealt with by information technology

(IT) security specialists. These specialists apply information security to technology (most often some form of computer system). It is worthwhile to note that a computer does not necessarily mean a home desktop.<sup>[27]</sup> A computer is any device with a *processor* and some memory. Such devices can range from non-networked standalone devices as simple as calculators, to networked mobile computing devices such as smartphones and tablet computers.<sup>[28]</sup> IT security specialists are almost always found in any major enterprise/establishment due to the nature and value of the data within larger businesses.<sup>[29]</sup> They are responsible for keeping all of the technology within the company secure from malicious cyber attacks that often attempt to acquire critical private information or gain control of the internal systems.<sup>[30][31]</sup>

The field of information security has grown and evolved significantly in recent years.<sup>[32]</sup> It offers many areas for specialization, including securing networks and allied infrastructure, securing applications and databases, security testing, information systems auditing, business continuity planning, electronic record discovery, and digital forensics.<sup>[33][34][35][36]</sup> Information security professionals are very stable in their employment.<sup>[37]</sup> As of 2013 more than 80 percent of professionals had no change in employer or employment over a period of a year, and the number of professionals is projected to continuously grow more than 11 percent annually from 2014 to 2019.<sup>[38]</sup>

**Threats**  [edit]

Information security threats come in many different forms.<sup>[39][40]</sup> Some of the most common threats today are software attacks, theft of intellectual property, theft of identity, theft of equipment or information, sabotage, and information extortion.<sup>[37][41]</sup> *Vipers*,<sup>[42]</sup> worms, phishing attacks, and Trojan horses are a few common examples of software attacks. The theft of intellectual property has also been an extensive issue for many businesses in the information technology (IT) field.<sup>[43]</sup> Identity theft is the attempt to act as someone else usually to obtain that person's personal information or to take advantage of their access to vital information through social engineering.<sup>[44][45]</sup> Theft of equipment or information is becoming more prevalent today due to the fact that most devices today are mobile.<sup>[46]</sup> are prone to theft and have also become far more desirable as the amount of data capacity increases. Sabotage usually consists of the destruction of an organization's website in an attempt to cause loss of confidence on the part of its customers.<sup>[44]</sup> Information extortion consists of theft of a company's property or information as an attempt to receive a payment in exchange for returning the information or property back to its owner, as with ransomware.<sup>[45]</sup> There are many ways to help protect yourself from some of these attacks but one of the most functional precautions is conduct periodic user awareness.<sup>[46]</sup> The number one threat to any organisation are users or internal employees, they are also called insider threats.<sup>[47]</sup>

Governments, military, corporations, financial institutions, hospitals, non-profit organisations, and private businesses amass a great deal of confidential information about their employees, customers, products, research, and financial status.<sup>[48]</sup> Should confidential information about a business's customers or finances or new product line fall into the hands of a competitor or a black hat hacker, a business and its customers could suffer widespread, irreparable financial loss, as well as damage to the company's reputation.<sup>[49]</sup> From a business perspective, information security must be balanced against cost, the Gordon-Loeb Model provides a mathematical economic approach for addressing this concern.<sup>[50]</sup>

For the individual, information security has a significant effect on privacy, which is viewed very differently in various cultures.<sup>[51]</sup>

**Responses to threats**  [edit]

Possible responses to a security threat or risk are:<sup>[52]</sup>

- reduce/mitigate – implement safeguards and countermeasures to eliminate vulnerabilities or block threats
- assign/transfer – place the cost of the threat onto another entity or organization such as purchasing insurance or outsourcing
- accept – evaluate if the cost of the countermeasure outweighs the possible cost of loss due to the threat.<sup>[53]</sup>

**History**  [edit]

Since the early days of communication, diplomats and military commanders understood that it was necessary to provide some mechanism to protect the confidentiality of correspondence and to have some means of detecting tampering.<sup>[54]</sup> Julius Caesar is credited with the invention of the Caesar cipher c. 50 B.C., which was created in order to prevent his secret messages from being read should a message fall into the wrong hands.<sup>[55]</sup> However, for the most part protection was achieved through the application of procedural handling controls.<sup>[40][56]</sup> Sensitive information was marked up to indicate that it should be protected and transported by trusted persons, guarded and stored in a secure environment or strong box.<sup>[57]</sup> As postal services expanded, governments created official organizations to intercept, decipher, read, and re-send letters (e.g., the U.K.'s Secret Office, founded in 1653<sup>[58]</sup>).

In the mid-nineteenth century more complex classification systems were developed to allow governments to manage their information according to the degree of sensitivity.<sup>[59]</sup> For example, the British Government codified this, to some extent, with the publication of the Official Secrets Act in 1888.<sup>[60]</sup> Section 1 of the law concerned espionage and unlawful disclosures of information, while Section 2 dealt with breaches of official trust.<sup>[61]</sup> A public interest defense was soon added to defend disclosures in the interest of the state.<sup>[62]</sup> A similar law was passed in India in 1859. The Indian Official Secrets Act, which was associated with the British colonial era and used to crack down on newspapers that opposed the Raj's policies.<sup>[63]</sup> A newer version was passed in 1923 that extended to all matters of confidential or secret information for governance.<sup>[64]</sup> By the time of the First World War, multi-tier classification systems were used to communicate information to and from various fronts, which encouraged greater use of code making and breaking sections in diplomatic and military headquarters.<sup>[65]</sup> Encoding became more sophisticated between the wars as machines were employed to scramble and unscramble information.<sup>[66]</sup>

The establishment of computer security inaugurated the history of information security. The need for such appeared during World War II.<sup>[68]</sup> The volume of information shared by the Allied countries during the Second World War necessitated formal alignment of classification systems and procedural controls.<sup>[69]</sup> An arcane range of markings evolved to indicate who could handle documents (usually officers rather than enlisted troops) and where they should be stored as increasingly complex safes and storage facilities were developed.<sup>[70]</sup> The Enigma Machine, which was employed by the Germans to encrypt the data of warfare and was successfully decrypted by Alan Turing, can be regarded as a striking example of creating and using secured information.<sup>[71]</sup> Procedures evolved to ensure documents were destroyed properly, and it was the failure to follow these procedures which led to some of the greatest intelligence coups of the war (e.g., the capture of U-570<sup>[72]</sup>).

Various Mainframe computers were connected online during the Cold War to complete more sophisticated tasks, in a communication process easier than mailing magnetic tapes back and forth by computer centers. As such, the Advanced Research Projects Agency (ARPA), of the United States Department of Defense, started researching the feasibility of a networked system of communication to trade information within the United States Armed Forces. In 1968, the ARPANET project was formulated by Dr. Larry Roberts, which would later evolve into what is known as the internet.<sup>[73]</sup>

In 1973, important elements of ARPANET security were found by internet pioneer Robert Metcalfe to have many flaws such as the "vulnerability of passwored structure and formats, lack of safety procedures for dial-up connections, and nonexistent user identification and authorizations", aside from the lack of controls and safeguards to keep data safe from unauthorized access. Hackers had effortless access to ARPANET, as phone numbers were known by the public.<sup>[74]</sup> Due to these problems, coupled with the constant violation of computer security, as well as the exponential increase in the number of hosts and users of the system, "network security" was often alluded to as "network insecurity".<sup>[75]</sup>

- Threats*
- Business continuity
- Laws and regulations
- Culture
- Sources of standards
- See also
- References
- Further reading*
- External links

- Threats*
- Business continuity
- Laws and regulations
- Culture
- Sources of standards
- See also

- References
- >Further reading
- External links

- Business continuity
- Laws and regulations
- Culture
- Sources of standards
- See also
- References
- >Further reading
- External links

The end of the twentieth century and the early years of the twenty-first century saw rapid advancements in telecommunications, computing hardware and software, and data encryption.<sup>[14]</sup> The availability of smaller, more powerful, and less expensive computing equipment made electronic data processing within the reach of small business and home users.<sup>[15]</sup> The establishment of Transfer Control Protocol/Internetwork Protocol (TCP/IP) in the early 1980s enabled different types of computers to communicate.<sup>[16]</sup> These computers quickly became interconnected through the internet.<sup>[17]</sup>

The rapid growth and widespread use of electronic data processing and electronic business conducted through the internet, along with numerous occurrences of international terrorism, fueled the need for better methods of protecting the computers and the information they store, process, and transmit.<sup>[18]</sup> The academic disciplines of computer security and information assurance emerged along with numerous professional organizations, all sharing the common goals of ensuring the security and reliability of information systems.<sup>[19][20][21][22]</sup>

Basic principles  [edit]

Key concepts  [edit]

The "CIA" triad of confidentiality, integrity, and availability is at the heart of information security.<sup>[23]</sup> (The members of the classic InfoSec triad—confidentiality, integrity, and availability—are interchangeably referred to in the literature as security attributes, properties, security goals, fundamental aspects, information criteria, critical information characteristics and basic building blocks.<sup>[24]</sup> However, debate continues about whether or not this triad is sufficient to address rapidly changing technology and business requirements, with recommendations to consider expanding on the intersections between availability and confidentiality, as well as the relationship between security and privacy.<sup>[25]</sup> Other principles such as "accountability" have sometimes been proposed. It has been pointed out that issues such as non-reputation do not fit well within the three core concepts.<sup>[26]</sup>

The triad seems to have first been mentioned in a NIST publication in 1977.<sup>[27]</sup>

In 1992 and revised in 2002, the OECD's *Guidelines for the Security of Information Systems and Networks*<sup>[28]</sup> proposed the nine generally accepted principles: awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management, and reassessment.<sup>[29]</sup> Building upon those, in 2004 the NIST's *Engineering Principles for Information Technology Security*<sup>[30]</sup> proposed 33 principles. From each of these derived guidelines and practices.

In 1998, Donn Parker proposed an alternative model for the classic "CIA" triad that he called the six atomic elements of information. The elements are confidentiality, possession, integrity, authenticity, availability, and utility. The merits of the *Palenstian Hexad* are a subject of debate amongst security professionals.<sup>[31]</sup>

In 2011, The Open Group published the information security management standard O-ISM,<sup>[32]</sup> This standard proposed an operational definition of the key concepts of security, with elements called "security objectives", related to access control (9), availability (3), data quality (1), compliance, and technical (4). In 2009, DoD Software Protection Initiative ( Archived 2016-09-25 at the Wayback Machine released the Three Tenets of Cybersecurity? Archived 2020-05-10 at the Wayback Machine which are System Susceptibility, Access to the Flaw, and Capability to Exploit the Flaw.<sup>[33][34][35]</sup> Neither of these models are widely adopted.

Confidentiality  [edit]

In information security, confidentiality "is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes."<sup>[36]</sup> While similar to "privacy," the two words are not interchangeable. Rather, confidentiality is a component of privacy that implements to protect our data from unauthorized viewers.<sup>[37]</sup> Examples of confidentiality of electronic data being compromised include laptop theft, password theft, or sensitive emails being sent to the incorrect individuals.<sup>[38]</sup>

Integrity  [edit]

In IT security, data integrity means maintaining and assuring the accuracy and completeness of data over its entire lifecycle.<sup>[39]</sup> This means that data cannot be modified in an unauthorized or undetected manner.<sup>[40]</sup> This is not the same thing as *referential integrity* in databases, although it can be viewed as a special case of consistency as understood in the classic ACID model of transaction processing.<sup>[41]</sup> Information security systems typically incorporate controls to ensure their own integrity, in particular protecting the kernel or core functions against both deliberate and accidental threats.<sup>[42]</sup> Multi-purpose and multi-user computer systems aim to compartmentalize the data and processing such that no user or process can adversely impact another; the controls may not succeed however, as we see in incidents such as malware infections, hacks, data theft, fraud, and privacy breaches.<sup>[43]</sup>

More broadly, integrity is an information security principle that involves human/social, process, and commercial integrity, as well as data integrity. As such it touches on aspects such as credibility, consistency, truthfulness, completeness, accuracy, timeliness, and assurance.<sup>[44]</sup>

Availability  [edit]

For any information system to serve its purpose, the information must be available when it is needed.<sup>[45]</sup> This means the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly.<sup>[46]</sup> High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades.<sup>[47]</sup> Ensuring availability also involves preventing denial-of-service attacks, such as a flood of incoming messages to the target system, essentially forcing it to shut down.<sup>[48]</sup>

In the realm of information security, availability can often be viewed as one of the most important parts of a successful information security program.<sup>[49][50][51][52][53][54]</sup> Ultimately and users need to be able to perform job functions; by ensuring availability, an organization is able to perform to the standards that an organization's stakeholders expect.<sup>[55]</sup> This can involve topics such as proxy configurations, outside web access, the ability to access shared drives and the ability to send emails.<sup>[56]</sup> Executives oftentimes do not understand the technical side of information security and look at availability as an easy fix, but this often requires collaboration from many different organizational teams, such as network operations, development operations, incident response, and policy/change management.<sup>[57]</sup> A successful information security team involves many different key roles to mesh and align for the "CIA" triad to be provided effectively.<sup>[58]</sup>

Non-reputation  [edit]





- Business continuity
- Laws and regulations
- Culture
- Sources of standards
- See also
- References
- Further reading
- External links



- Business continuity
- Laws and regulations
- Culture
- Sources of standards
- See also
- References
- Further reading
- External links

in law, non-repudiation imposes one a mention to turn their obligations to a contract, it also implies that one party or a transaction cannot deny having received a transaction, nor can the other party deny having sent a transaction.<sup>[1][2]</sup>

It is important to note that while technology such as cryptographic systems can assist in non-repudiation efforts, the concept is at its core a legal concept transcending the realm of technology.<sup>[1][3]</sup> It is not, for instance, sufficient to show that the message matches a digital signature signed with the sender's private key, and thus only the sender could have sent the message, and nobody else could have altered it in transit (*data integrity*).<sup>[1][3]</sup> The alleged sender could in return demonstrate that the digital signature algorithm is vulnerable or flawed, or allege or prove that his signing key has been compromised.<sup>[1][3]</sup> The fault for these violations may or may not lie with the sender, and such assertions may or may not relieve the sender of liability, but the assertion would invalidate the claim that the signature necessarily proves authenticity and integrity. As such, the sender may repudiate the message (because authenticity and integrity are pre-requisites for non-repudiation).<sup>[1][3]</sup>

## Risk management

Main article: *Risk management*

Broadly speaking, risk is the likelihood that something bad will happen that causes harm to an informational asset (or the loss of the asset).<sup>[1][2]</sup> A vulnerability is a weakness that could be used to endanger or cause harm to an informational asset. A threat is anything (man-made or act of nature) that has the potential to cause harm.<sup>[1][2]</sup> The likelihood that a threat will use a vulnerability to cause harm creates a risk. When a threat does use a vulnerability to inflict harm, it has an impact.<sup>[1][4]</sup> In the context of information security, the impact is a loss of availability, integrity, and confidentiality, and possibly other losses (lost income, loss of life, loss of real property).<sup>[1][4]</sup>

The *Certified Information Systems Auditor (CISA) Review Manual* 2006 defines **risk management** as "the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures,<sup>[1][5]</sup> if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization."<sup>[1][7]</sup>

There are two things in this definition that may need some clarification. First, the process of risk management is an ongoing, iterative process. It must be repeated indefinitely. The business environment is constantly changing and new threats and vulnerabilities emerge every day.<sup>[1][8]</sup> Second, the choice of countermeasures (controls) used to manage risks must strike a balance between productivity, cost, effectiveness of the countermeasure, and the value of the informational asset being protected.<sup>[1][16]</sup> Furthermore, these processes have limitations as security breaches are generally rare and emerge in a specific context which may not be easily duplicated.<sup>[1][2]</sup> Thus, any process and countermeasure should itself be evaluated for vulnerabilities.<sup>[1][2]</sup> It is not possible to identify all risks, nor is it possible to eliminate all risk. The remaining risk is called "residual risk."<sup>[1][9]</sup>

A risk assessment is carried out by a team of people who have knowledge of specific areas of the business.<sup>[1][1]</sup> Membership of the team may vary over time as different parts of the business are assessed.<sup>[1][1]</sup> The assessment may use a subjective qualitative analysis based on informed opinion, or where reliable dollar figures and historical information is available, the analysis may use quantitative analysis.

Research has shown that the most vulnerable point in most information systems is the human user, operator, designer, or other human.<sup>[1][2]</sup> The ISO/IEC 27002:2005 Code of practice for information security management recommends the following be examined during a risk assessment:

- security policy;
- organization of information security;
- asset management;
- human resources security;
- physical and environmental security;
- communications and operations management;
- access control;
- information systems acquisition, development, and maintenance;
- information security incident management;
- business continuity management;
- regulatory compliance.

In broad terms, the risk management process consists of:<sup>[1][26][12]</sup>

1. Identification of assets and estimating their value. Include: people, buildings, hardware, software, data (electronic, print, other), supplies.<sup>[1][26]</sup>
2. Conduct a threat assessment. Include: Acts of nature, acts of war, accidents, malicious acts originating from inside or outside the organization.<sup>[1][26]</sup>
3. Conduct a vulnerability assessment, and for each vulnerability, calculate the probability that it will be exploited. Evaluate policies, procedures, standards, training, physical security, quality control, technical security.<sup>[1][26]</sup>
4. Calculate the impact that each threat would have on each asset. Use qualitative analysis or quantitative analysis.<sup>[1][2]</sup>
5. Identify, select and implement appropriate controls. Provide a proportional response. Consider productivity, cost effectiveness, and value of the asset.<sup>[1][32]</sup>
6. Evaluate the effectiveness of the control measures. Ensure the controls provide the required cost effective protection without discernible loss of productivity.<sup>[1][33]</sup>

For any given risk, management can choose to accept the risk based upon the relative low value of the asset, the relative low frequency of occurrence, and the relative low impact on the business.<sup>[1][1]</sup> Or, leadership may choose to mitigate the risk by selecting and implementing appropriate control measures to reduce the risk. In some cases, the risk can be transferred to another business by buying insurance or outsourcing to another business.<sup>[1][10]</sup> The reality of some risks may be disputed. In such cases leadership may choose to deny the risk.<sup>[1][16]</sup>

## Security controls

Main article: *security controls*

Selecting and implementing proper security controls will initially help an organization bring down risk to acceptable levels.<sup>[1][17]</sup> Control selection should follow and should be based on the risk assessment.<sup>[1][18]</sup> Controls can vary in nature, but fundamentally they are ways of protecting the confidentiality, integrity or availability of information. ISO/IEC 27001 has defined controls in different areas.<sup>[1][18]</sup> Organizations can implement additional controls according to requirement of the organization.<sup>[1][40]</sup> ISO/IEC 27002 offers a guideline for organizational information security standards.<sup>[1][41]</sup>

## Administrative

Administrative controls (also called procedural controls) consist of approved written policies, procedures, standards, and guidelines. Administrative controls

- Business continuity
- Laws and regulations
- Culture
- Sources of standards
- See also
- References
- Further reading
- External links

- Business continuity

There are frameworks for running an business and managing people. They ensure people on how the business is to be run and how day-to-day operations are to be conducted. Laws and regulations created by government bodies are also a type of administrative control because they inform the business.<sup>[143]</sup> Some industry sectors have policies, procedures, standards, and guidelines that must be followed – the Payment Card Industry Data Security Standard<sup>[144]</sup> (PCI DSS) required by Visa and MasterCard is such an example. Other examples of administrative controls include the corporate security policy, password policy, hiring policies, and disciplinary policies.<sup>[145]</sup>

Administrative controls form the basis for the selection and implementation of logical and physical controls. Logical and physical controls are manifestations of administrative controls, which are of paramount importance.<sup>[146]</sup>

#### Logical

Logical controls (also called technical controls) use software and data to monitor and control access to information and computing systems.<sup>[147] [148] [149]</sup> Passwords, network and host-based firewalls, network intrusion detection systems, access control lists, and data encryption are examples of logical controls.<sup>[145]</sup>

An important logical control that is frequently overlooked is the principle of least privilege, which requires that an individual, program or system process not be granted any more access privileges than are necessary to perform the task.<sup>[147]</sup> A blatant example of the failure to adhere to the principle of least privilege is logging into Windows as user Administrator to read email and surf the web. Violations of this principle can also occur when an individual collects additional access privileges over time.<sup>[148]</sup> This happens when employees' job duties change, employees are promoted to a new position, or employees are transferred to another department.<sup>[149]</sup> The access privileges required by their new duties are frequently added onto their already existing access privileges, which may no longer be necessary or appropriate.<sup>[150]</sup>

#### Physical

Physical controls monitor and control the environment of the work place and computing facilities.<sup>[151] [152]</sup> They also monitor and control access to and from such facilities and include doors, locks, heating and air conditioning, smoke and fire alarms, fire suppression systems, cameras, barricades, fencing, security guards, cable locks, etc. Separating the network and workplace into functional areas are also physical controls.<sup>[153]</sup>

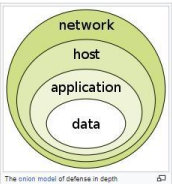
An important physical control that is frequently overlooked is separation of duties, which ensures that an individual can not complete a critical task by himself.<sup>[153]</sup> For example, an employee who submits a request for reimbursement should not also be able to authorize payment or print the check.<sup>[154]</sup> An applications programmer should not also be the server administrator or the database administrator; these roles and responsibilities must be separated from one another.<sup>[155]</sup>

#### Defense in depth

Main article: *Defense in depth (computing)*

Information security must protect information throughout its lifespan, from the initial creation of the information on through to the final disposal of the information.<sup>[156]</sup> The information must be protected while in motion and while at rest. During its lifetime, information may pass through many different information processing systems and through many different parts of information processing systems.<sup>[157]</sup> There are many different ways the information and information systems can be threatened. To fully protect the information during its lifetime, each component of the information processing system must have its own protection mechanisms.<sup>[158]</sup> The building up, layering on, and overlapping of security measures is called "defense in depth."<sup>[159]</sup> In contrast to a metal chain, which is famously only as strong as its weakest link, the defense in depth strategy aims at a structure where, should one defensive measure fail, other measures will continue to provide protection.<sup>[160]</sup>

Recall the earlier discussion about administrative controls, logical controls, and physical controls. The three types of controls can be used to form the basis upon which to build a defense in depth strategy.<sup>[161]</sup> With this approach, defense in depth can be conceptualized as three distinct layers or planes laid one on top of the other.<sup>[162]</sup> Additional insight into defense in depth can be gained by thinking of it as forming the layers of an onion, with data at the core of the onion, people the next outer layer of the onion, and network security, host-based security, and application security forming the outermost layers of the onion.<sup>[163]</sup> Both perspectives are equally valid, and each provides valuable insight into the implementation of a good defense in depth strategy.<sup>[164]</sup>



#### Classification

An important aspect of information security and risk management is recognizing the value of information and defining appropriate procedures and protection requirements for the information.<sup>[164]</sup> Not all information is equal and so not all information requires the same degree of protection.<sup>[165]</sup> This requires information to be assigned a security classification.<sup>[166]</sup> The first step in information classification is to identify a member of senior management as the owner of the particular information to be classified. Next, develop a classification policy.<sup>[167]</sup> The policy should describe the different classification labels, define the criteria for information to be assigned a particular label, and list the required security controls for each classification.<sup>[168]</sup>

Some factors that influence which classification information should be assigned include how much value that information has to the organization, how old the information is and whether or not the information has become obsolete.<sup>[169]</sup> Laws and other regulatory requirements are also important considerations when classifying information.<sup>[170]</sup> The Information Systems Audit and Control Association (ISACA) and its *Business Model for Information Security* also serves as a tool for security professionals to examine security from a systems perspective, creating an environment where security can be managed holistically, allowing actual risks to be addressed.<sup>[171]</sup>

The type of information security classification labels selected and used will depend on the nature of the organization, with examples being<sup>[168]</sup>

- In the business sector, labels such as: Public, Sensitive, Private, Confidential.
- In the government sector, labels such as: Unclassified, Unofficial, Protected, Confidential, Secret, Top Secret, and their non-English equivalents.<sup>[172]</sup>
- In cross-sectoral formations, the Traffic Light Protocol, which consists of White, Green, Amber, and Red.
- In the personal sector, one label such as Financial. This includes activities related to managing money, such as online banking.<sup>[173]</sup>

All employees in the organization, as well as business partners, must be trained on the classification schema and understand the required security controls and handling procedures for each classification.<sup>[174]</sup> The classification of a particular information asset that has been assigned should be reviewed periodically to ensure the classification is still appropriate for the information and to ensure the security controls required by the classification are in place and are followed in their right procedures.<sup>[175]</sup>



- Laws and regulations
- Culture
- Sources of standards
- See also
- References
- >Further reading
- External links

**Access control** [ edit ]

Access to protected information must be restricted to people who are authorized to access the information.<sup>[1][2]</sup> The computer programs, and in many cases the computers that process the information, must also be authorized.<sup>[1][2]</sup> This requires that mechanisms be in place to control the access to protected information.<sup>[1][2]</sup> The sophistication of the access control mechanisms should be in parity with the value of the information being protected; the more sensitive or valuable the information the stronger the control mechanisms need to be.<sup>[1][2]</sup> The foundation on which access control mechanisms are built start with identification and authentication.<sup>[1][2]</sup>

Access control is generally considered in three steps: identification, authentication, and authorization.<sup>[1][2][3]</sup>

**Identification** [ edit ]

Identification is an assertion of who someone is or what something is. If a person makes the statement "Hello, my name is John Doe" they are making a claim of who they are.<sup>[1][1]</sup> However, their claim may or may not be true. Before John Doe can be granted access to protected information it will be necessary to verify that the person claiming to be John Doe really is John Doe.<sup>[1][2]</sup> Typically the claim is in the form of a username. By entering that username you are claiming "I am the person the username belongs to."<sup>[1][3]</sup>

**Authentication** [ edit ]

Authentication is the act of verifying a claim of identity. When John Doe goes into a bank to make a withdrawal, he tells the bank teller he is John Doe, a claim of identity.<sup>[1][4]</sup> The bank teller asks to see a photo ID, so he hands the teller his *driver's license*.<sup>[1][4]</sup> The bank teller checks the license to make sure it has John Doe printed on it and compares the photograph on the license against the person claiming to be John Doe.<sup>[1][4]</sup> If the photo and name match the person, then the teller has authenticated that John Doe is who he claimed to be. Similarly, by entering the correct password, the user is providing evidence that he/she is the person the username belongs to.<sup>[1][5]</sup>

There are three different types of information that can be used for authentication:<sup>[1][3][1][6]</sup>

- Something you know: things such as a PIN, a *password*, or your mother's maiden name<sup>[1][3][1][7]</sup>
- Something you have: a driver's license or a magnetic swipe card<sup>[1][3][1][8]</sup>
- Something you are: *biometrics*, including palm prints, fingerprints, voice prints, and retina (eye) scans<sup>[1][4]</sup>

Strong authentication requires providing more than one type of authentication information (two-factor authentication).<sup>[1][9]</sup> The username is the most common form of identification on computer systems today and the password is the most common form of authentication.<sup>[1][9]</sup> Usernames and passwords have served their purpose, but they are increasingly inadequate.<sup>[1][7]</sup> Usernames and passwords are slowly being replaced or supplemented with more sophisticated authentication mechanisms such as Time-based One-time Password algorithms.<sup>[1][10]</sup>

**Authorization** [ edit ]

After a person, program or computer has successfully been identified and authenticated then it must be determined what informational resources they are permitted to access and what actions they will be allowed to perform (run, view, create, delete, or change).<sup>[1][11]</sup> This is called authorization. Authorization to access information and other computing services begins with administrative policies and procedures.<sup>[1][11]</sup> The policies prescribe what information and computing services can be accessed, by whom, and under what conditions. The access control mechanisms are then configured to enforce these policies.<sup>[1][11]</sup> Different computing systems are equipped with different kinds of access control mechanisms. Some may even offer a choice of different access control mechanisms.<sup>[1][12]</sup> The access control mechanism a system offers will be based upon one of three approaches to access control, or it may be derived from a combination of the three approaches.<sup>[1][12]</sup>

The non-discretionary approach consolidates all access control under a centralized administration.<sup>[1][12]</sup> The access to information and other resources is usually based on the individuals function (role) in the organization or the tasks the individual must perform.<sup>[1][12][1][13]</sup> The discretionary approach gives the creator or owner of the information resource the ability to control access to those resources.<sup>[1][13]</sup> In the mandatory access control approach, access is granted or denied basing upon the security classification assigned to the information resource.<sup>[1][14]</sup>

Examples of common access control mechanisms in use today include role-based access control, available in many advanced database management systems; simple file permissions provided in the UNIX and Windows operating systems;<sup>[1][15]</sup> Group Policy Objects provided in Vindovs network systems; and Kerberos, RADIUS, TACACS, and the simple access lists used in many firewalls and routers.<sup>[1][16]</sup>

To be effective, policies and other security controls must be enforceable and upheld. Effective policies ensure that people are held accountable for their actions.<sup>[1][17]</sup> The U.S. *Treasury's* guidelines for systems processing sensitive or proprietary information, for example, states that all failed and successful authentication and access attempts must be logged, and all access to information must leave some type of audit trail.<sup>[1][18]</sup>

Also, the need-to-know principle needs to be in effect when talking about access control. This principle gives access rights to a person to perform their job functions.<sup>[1][19]</sup> This principle is used in the government when dealing with difference clearances.<sup>[1][1]</sup> Even though two employees in different departments have a top-secret clearance, they must have a need-to-know in order for information to be exchanged. Within the need-to-know principle, network administrators grant the employee the least amount of privilege to prevent employees from accessing more than what they are supposed to.<sup>[1][19]</sup> Need-to-know helps to enforce the confidentiality-integrity-availability triad. Need-to-know directly impacts the confidential area of the triad.<sup>[1][20]</sup>

**Cryptography** [ edit ]

*Main article: Cryptography*

Information security uses *cryptography* to transform usable information into a form that renders it unusable by anyone other than an authorized user; this process is called *encryption*.<sup>[1][21]</sup> Information that has been encrypted (rendered unusable) can be transformed back into its original usable form by an authorized user who possesses the *cryptographic key*, through the process of decryption.<sup>[1][21]</sup> Cryptography is used in information security to protect information from unauthorized or accidental disclosure while the information is in transit (either electronically or physically) and while information is in storage.<sup>[1][2]</sup>

Cryptography provides information security with other useful applications as well, including improved authentication methods, message digests, digital signatures, non-repudiation, and encrypted network communications.<sup>[1][1]</sup> Older, less secure applications such as Telnet and File Transfer Protocol (FTP) are slowly being replaced with more secure applications such as Secure Shell (SSH) that use encrypted network communications.<sup>[1][1]</sup> Wireless communications can be encrypted using protocols such as WPA/WPA2, or the older (and less secure) WEP. Wired communications (such as TLU-T G In) are secured using AES for encryption and X.1035 for authentication and key exchange.<sup>[1][12]</sup> Software applications such as GnuPG or PGP can be used to encrypt data files and email.<sup>[1][16]</sup>

Cryptography can introduce security problems when it is not implemented correctly.<sup>[1][22]</sup> Cryptographic solutions need to be implemented using industry-standard solutions that have undergone rigorous peer review for independent verifiability in mathematics.<sup>[1][23]</sup> The security and integrity of this information has to

*LOCKDOWN*

- Business continuity
- Laws and regulations
- Culture
- Sources of standards
- See also
- References
- >Further reading
- External links

- Business continuity
- Laws and regulations
- Culture
- Sources of standards
- See also
- References
- Further reading
- External links

Business continuity

Plans and regulations

Culture

Sources of standards

See also

References

Further reading

External links

Business continuity

This is where the threat that was identified is removed from the affected systems [344] This could include deleting malicious files, terminating compromised accounts, or deleting other components [345][346] Some events do not require this step, however it is important to fully understand the event before moving to this step [347] This will help to ensure that the threat is completely removed [348]

Recovery [ edit ]

This stage is where the systems are restored back to original operation [349] This stage could include the recovery of data, changing user access information, or updating firewall rules or policies to prevent a breach in the future [350][351] Without enclosing this step, the system could still be vulnerable to future security threats [352]

Lessons Learned [ edit ]

In this step information that has been gathered during this process is used to make future decisions on security [353] This step is crucial to the ensure that future events are prevented. Using this information to further train admins is critical to the process [354] This step can also be used to process information that is distributed from other entities who have experienced a security event [343]

Change management [ edit ]

Main article: *Change Management (ITSM)*

Change management is a formal process for directing and controlling alterations to the information processing environment [344][345] This includes alterations to desktop computers, the network, servers, and software [344] The objectives of change management are to reduce the risks posed by changes to the information processing environment and improve the stability and reliability of the processing environment as changes are made [347] It is not the objective of change management to prevent or hinder necessary changes from being implemented [350][351]

Any change to the information processing environment introduces an element of risk [370] Even apparently simple changes can have unexpected effects [371] One of management's many responsibilities is the management of risk [372][373] Change management is a tool for managing the risks introduced by changes to the information processing environment [374] Part of the change management process ensures that changes are not implemented at inopportune times when they may disrupt critical business processes or interfere with other changes being implemented [375]

Not every change needs to be managed [374][377] Some kinds of changes are a part of the everyday routine of information processing and adhere to a predefined procedure, which reduces the overall level of risk to the processing environment [376] Creating a new user account or deploying a new desktop computer are examples of changes that do not generally require change management [378] However, installing user file shares, or upgrading the email server pose a much higher level of risk to the processing environment and are not a normal everyday activity [380] The critical first steps in change management are (a) defining change (and communicating that definition) and (b) defining the scope of the change system [381]

Change management is usually overseen by a change review board composed of representatives from key business areas, [342] security, networking, systems administrators, database administration, application developers, desktop support, and the help desk [383] The tasks of the change review board can be facilitated with the use of automated work flow application [384] The responsibility of the change review board is to ensure the organization's documented change management procedures are followed [385] The change management process is as follows[386]

- Request: Anyone can request a change [379][380] The person making the change request may or may not be the same person that performs the analysis or implements the change [374][383] When a request for change is received, it may undergo a preliminary review to determine if the requested change is compatible with the organization's business model and practices, and to determine the amount of resources needed to implement the change [391]
- Approve: Management runs the business and controls the allocation of resources therefore, management must approve requests for changes and assign a priority for every change [392] Management might choose to reject a change request if the change is not compatible with the business model, industry standards or best practices [393][394] Management might also choose to reject a change request if the change requires more resources than can be allocated for the change [395]
- Plan: Planning a change involves discovering the scope and impact of the proposed change, analyzing the complexity of the change, allocation of resources and, developing, testing, and documenting both implementation and back-out plans [396] Need to define the criteria on which a decision to back out will be made [397]
- Test: Every change must be tested in a safe test environment, which closely reflects the actual production environment, before the change is applied to the production environment [398] The backout plan must also be tested [399]
- Schedule: Part of the change review board's responsibility is to assist in the scheduling of changes by reviewing the proposed implementation date for potential conflicts with other scheduled changes or critical business activities [400]
- Communicate: Once a change has been scheduled it must be communicated [343] The communication is to give others the opportunity to remind the change review board about other changes or critical business activities that might have been overlooked when scheduling the change [392] The communication also serves to make the help desk and users aware that a change is about to occur [394] Another responsibility of the change review board is to ensure that scheduled changes have been properly communicated to those who will be affected by the change or otherwise have an interest in the change [344][346]
- Implement: At the appointed date and time, the changes must be implemented [398][347] Part of the planning process was to develop an implementation plan, testing plan and, a back out plan [346][399] If the implementation of the change should fail or, the post implementation testing fails or, other "drop dead" criteria have been met, the back out plan should be implemented [395]
- Document: All changes must be documented [371][373] The documentation includes the initial request for change, its approval, the priority assigned to it, the implementation [370] testing and back out plans, the results of the change review board critique, the date/time the change was implemented, [374] who implemented it, and whether the change was implemented successfully, failed or postponed [373][374]
- Post-change review: The change review board should hold a post-implementation review of changes [373] It is particularly important to review failed and backed out changes. The review board should try to understand the problems that were encountered, and look for areas for improvement. [377]

Change management procedures that are simple to follow and easy to use can greatly reduce the overall risks created when changes are made to the information processing environment [378] Good change management procedures improve the overall quality and success of changes as they are implemented [378] This is accomplished through planning, peer review, documentation, and communication [390]

ISO/IEC 20000, The Visible OPS Handbook: Implementing ITIL in 4 Practical and Auditable Steps[401] (Full book summary), [402] and ITIL all provide valuable guidance on implementing an efficient and effective change management program information security [353]

Business continuity



Business continuity management (BCM) concerns arrangements aiming to protect an organization's critical business functions from interruption due to incidents, or at least minimise the effects.<sup>[a][b][c]</sup> BCM is essential to any organization to keep technology and business in line with current threats to the continuation of business as usual.<sup>[a]</sup> The BCM should be included in an organizations risk analysis plan to ensure that all of the necessary business functions have what they need to keep going in the event of any type of threat to any business function.<sup>[a][7]</sup>

It encompasses:

- Analysis of requirements, e.g., identifying critical business functions, dependencies and potential failure points, potential threats and hence incidents or risks of concern to the organization.<sup>[a][8][24]</sup>
- Specification, e.g., maximum tolerable outage periods; recovery point objectives (maximum acceptable periods of data loss).<sup>[24]</sup>
- Architecture and design, e.g., an appropriate combination of approaches including resilience (e.g. engineering IT systems and processes for high availability),<sup>[21]</sup> avoiding or preventing situations that might interrupt the business), incident and emergency management (e.g., evacuating premises, calling the emergency services, triage/situation)<sup>[22]</sup> assessment and invoking recovery plans), recovery (e.g., rebuilding) and contingency management (generic capabilities to deal positively with whatever occurs using whatever resources are available).<sup>[23][2]</sup>
- Implementation, e.g., configuring and scheduling backups, data transfers, etc., duplicating and strengthening critical elements; contracting with service and equipment suppliers;
- Testing, e.g., business continuity exercises of various types, costs and assurance levels.<sup>[24]</sup>
- Management, e.g., defining strategies, setting objectives and goals; planning and directing the work; allocating funds, people and other resources; prioritization relative to other activities; team building, leadership, control, motivation and coordination with other business functions and activities<sup>[24]</sup> (e.g., IT, facilities, human resources, risk management, information risk and security, operations); monitoring the situation, checking and updating the arrangements when things change; maturing the approach through continuous improvement, learning and appropriate investment.<sup>[a][25][26][27]</sup>
- Assurance, e.g., testing against specified requirements; measuring, analyzing, and reporting key parameters; conducting additional tests, reviews and audits for greater confidence that the arrangements will go to plan if needed.<sup>[28]</sup>

Whereas BCM takes a broad approach to minimizing disaster-related risks by reducing both the probability and the severity of incidents, a disaster recovery plan (DRP) focuses specifically on resuming business operations as quickly as possible after a disaster.<sup>[1][7]</sup> A disaster recovery plan, invoked soon after a disaster occurs, lays out the steps necessary to recover critical information and communications technology (ICT) infrastructure.<sup>[1][29]</sup> Disaster recovery planning includes establishing a planning group, performing risk assessment, establishing priorities, developing recovery strategies, preparing inventories and documentation of the plan, developing verification criteria and procedure, and lastly implementing the plan.<sup>[1][24]</sup>

### Laws and regulations [edit]

Below is a partial listing of governmental laws and regulations in various parts of the world that have, had, or will have, a significant effect on data processing and information security.<sup>[a][30][31]</sup> Important industry sector regulations have also been included when they have a significant impact on information security.<sup>[24]</sup>

- The UK Data Protection Act 1998 makes new provisions for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.<sup>[1][32][33]</sup> The European Union Data Protection Directive (EUDD)<sup>[34]</sup> requires that all E.U. members adopt national regulations to standardize the protection of data privacy for citizens throughout the E.U.<sup>[34][35]</sup>
- The Computer Misuse Act 1990 is an Act of the U.K. Parliament making computer crime (e.g., hacking) a criminal offense.<sup>[34]</sup> The act has become a model upon which several other countries,<sup>[34]</sup> including Canada and the Republic of Ireland, have drawn inspiration from when subsequently drafting their own information security laws.<sup>[34][36]</sup>
- The E.U.'s Data Retention Directive (amulled) required internet service providers and phone companies to keep data on every electronic message sent and phone call made for between six months and two years.<sup>[36]</sup>
- The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232 (p.g. 34 CFR Part 99)) is a U.S. Federal law that protects the privacy of student education records.<sup>[34][37]</sup> The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.<sup>[34]</sup> Generally, schools must have written permission from the parent or eligible student<sup>[34][38][39]</sup> in order to release any information from a student's education record.<sup>[34]</sup>
- The Federal Financial Institutions Examination Council's (FFIEC) security guidelines for auditors specifies requirements for online banking security.<sup>[34]</sup>
- The Health Insurance Portability and Accountability Act (HIPAA) of 1996 requires the adoption of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.<sup>[34]</sup> Additionally, it requires health care providers, insurance providers and employers to safeguard the security and privacy of health data.<sup>[34]</sup>
- The Gramm–Leach–Bliley Act of 1999 (GLBA), also known as the Financial Services Modernization Act of 1999, protects the privacy and security of private financial information that financial institutions collect, hold, and process.<sup>[34]</sup>
- Section 404 of the Sarbanes–Oxley Act of 2002 (SOX) requires publicly traded companies to assess the effectiveness of their internal controls for financial reporting in annual reports they submit at the end of each fiscal year.<sup>[34]</sup> Chief information officers are responsible for the security, accuracy, and reliability of the systems that manage and report the financial data.<sup>[34]</sup> The act also requires publicly traded companies to engage with independent auditors who must attest to, and report on, the validity of their assessments.<sup>[34]</sup>
- The Payment Card Industry Data Security Standard (PCI DSS) establishes comprehensive requirements for enhancing payment account data security.<sup>[34]</sup> It was developed by the founding payment brands of the PCI Security Standards Council — including American Express, Discover, Financial Services, JCB, MasterCard Worldwide,<sup>[34]</sup> and Visa International — to help facilitate the broad adoption of consistent data security measures on a global basis.<sup>[34][4]</sup> The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures.<sup>[34]</sup>
- State security breach notification laws (California and many others) require businesses, nonprofits, and state institutions to notify consumers when unencrypted "personal information" may have been compromised, lost, or stolen.<sup>[34]</sup>
- The Personal Information Protection and Electronics Document Act (PIPEDA) of Canada supports and promotes electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances.<sup>[34][340]</sup> by providing for the use of electronic means to communicate or record information or transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act.<sup>[34][341][342]</sup>



<sup>[</sup><sup>]</sup>

- Greece's Hellenic Authority for Communication Security and Privacy (ADAE) (Law 165/2011) establishes and describes the minimum information security controls that should be deployed by every company which provides electronic communication networks and/or services in Greece in order to protect customers' confidentiality.<sup>[172]</sup> These include both managerial and technical controls (e.g., log records should be stored for two years).<sup>[173]</sup>
- Greece's Hellenic Authority for Communication Security and Privacy (ADAE) (Law 205/2013) concentrates around the protection of the integrity and availability of the services and data offered by Greek telecommunication companies.<sup>[174]</sup> The law forces these and other related companies to build, deploy, and test appropriate business continuity plans and redundant infrastructures.<sup>[175]</sup>

The US Department of Defense (DoD) issued DoD Directive 8570 in 2004, supplemented by DoD Directive 8140, requiring all DoD employees and all DoD contract personnel involved in information assurance roles and activities to earn and maintain various industry Information Technology (IT) certifications in an effort to ensure that all DoD personnel involved in network infrastructure defense have minimum levels of IT industry recognized knowledge, skills and abilities (KSA). Andersson and Reimers (2019) report these certifications range from CompTIA's A+ and Security+ through the ICS2.org's CISSP, etc. <sup>[176]</sup>

## Culture <sup>[</sup><sup>edit]</sup>

Describing more than simply how security aware employees are, information security culture is the ideas, customs, and social behaviors of an organization that impact information security in both positive and negative ways.<sup>[177]</sup> Cultural concepts can help different segments of the organization work effectively or work against effectiveness towards information security within an organization. The way employees think and feel about security and the actions they take can have a big impact on information security in organizations. Roer & Petric (2017) identify seven core dimensions of information security culture in organizations.<sup>[178]</sup>

- **Attitudes:** Employees' feelings and emotions about the various activities that pertain to the organizational security of information.<sup>[178]</sup>
- **Behaviors:** Actual or intended activities and risk-taking actions of employees that have direct or indirect impact on information security.
- **Cognition:** Employees' awareness, verifiable knowledge, and beliefs regarding practices, activities, and self-efficacy relation that are related to information security.
- **Communication:** Ways employees communicate with each other, sense of belonging, support for security issues, and incident reporting.
- **Compliance:** Adherence to organizational security policies, awareness of the existence of such policies and the ability to recall the substance of such policies.
- **Norms:** Perceptions of security-related organizational conduct and practices that are informally deemed either normal or deviant by employees and their peers, e.g., hidden expectations regarding security behaviors and unwritten rules regarding uses of information-communication technologies.
- **Responsibilities:** Employees' understanding of the roles and responsibilities they have as a critical factor in sustaining or endangering the security of information, and thereby the organization.

Andersson and Reimers (2014) found that employees often do not see themselves as part of the organization Information Security "effort" and often take actions that ignore organizational information security best interests.<sup>[180]</sup> Research shows information security culture needs to be improved continuously. In *Information Security Culture from Analysis to Change*, authors commented, "It's a never ending process, a cycle of evaluation and change or maintenance." To manage the information security culture, five steps should be taken: pre-evaluation, strategic planning, operative planning, implementation, and post-evaluation.<sup>[181]</sup>

- **Pre-Evaluation:** to identify the awareness of information security within employees and to analyze current security policy
- **Strategic Planning:** to come up a better awareness-program, we need to set clear targets. Clustering people is helpful to achieve it.
- **Operative Planning:** create a good security culture based on internal communication, management buy-in, security awareness, and training programs
- **Implementation:** should feature commitment of management, communication with organizational members, courses for all organizational members, and commitment of the employees<sup>[181]</sup>
- **Post-evaluation:** to better gauge the effectiveness of the prior steps and build on continuous improvement

## Sources of standards <sup>[</sup><sup>edit]</sup>

Main article: *Cyber Security Standards*

The International Organization for Standardization (ISO) is an international standards organization organized as a consortium of national standards institutions from 167 countries, coordinated through a secretariat in Geneva, Switzerland. ISO is the world's largest developer of international standards. The International Electrotechnical Commission (IEC) is an international standards organization that deals with electrotechnology and cooperates closely with ISO. ISO/IEC 15443: "Information technology – Security techniques – A framework for IT security assurance", ISO/IEC 27002: "Information technology – Security techniques – Code of practice for information security management", ISO/IEC 20000: "Information technology – Service management", and ISO/IEC 27031: "Information technology – Security techniques – Information security management systems – Requirements" are of particular interest to information security professionals.

The US National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the U.S. Department of Commerce. The NIST Computer Security Division develops standards, metrics, tests, and validation programs as well as publishes standards and guidelines to increase secure IT planning, implementation, management, and operation. NIST is also the custodian of the U.S. Federal Information Processing Standard publications (FIPS).

The Internet Society is a professional membership society with more than 100 organizations and over 20,000 individual members in over 100 countries. It provides leadership in addressing issues that confront the future of the Internet, and it is the organizational home for the groups responsible for Internet infrastructure standards, including the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB). The ISOC hosts the Requests for Comments (RFCs) which includes the Official Internet Protocol Standards and the RFC-2196 Site Security Handbook.

The Information Security Forum (ISF) is a global nonprofit organization of several hundred leading organizations in financial services, manufacturing, telecommunications, consumer goods, government, and other areas. It undertakes research into information security practices and offers advice in its biannual Standard of Good Practice and more detailed advisories for members.

The Institute of Information Security Professionals (ISPP) is an independent, non-profit body governed by its members, with the principal objective of advancing the professionalism of information security practitioners and thereby the professionalism of the industry as a whole. The institute developed the ISPP Skills Framework. This framework describes the range of competencies expected of information security and information assurance professionals in the effective performance of their roles. It was developed through collaboration between both private and public sector organizations, world-renowned academics, and security leaders.<sup>[182]</sup>

<sup>[</sup><sup>]</sup>

Business continuity

Laws and regulations

Culture

Sources of standards

See also

References

Further reading

External links

<sup>[</sup><sup>]</sup>

Business continuity

Laws and regulations

Culture

Sources of standards

See also

References

➤Further reading

External links

The German Federal Office for Information Security (in German *Bundesamt für Sicherheit in der Informationstechnik* (BSI) BSI-Standards 100-1 to 100-4 are a set of recommendations including "methods, processes, procedures, approaches and measures relating to information security"<sup>[1]</sup>. The BSI Standard 100-2 / IT-Grundschutz Methodology describes how information security management can be implemented and operated. The standard includes a very specific guide, the IT Baseline Protection Catalogs (also known as IT-Grundschutz Catalogs). Before 2005, the catalogs were formerly known as "IT Baseline Protection Manual". The Catalogs are a collection of documents useful for detecting and combating security-relevant weak points in the IT environment (IT cluster). The collection encompasses as of September 2013 over 4,400 pages with the introduction and catalogs. The IT-Grundschutz approach is signed with the ISO/IEC 27000 family.

The European Telecommunications Standards Institute standardized a catalog of information security indicators, headed by the Industrial Specification Group (ISG) ISI.

See also

- Backup
  - Capability-based security
  - Computer security (cybersecurity)
  - Data breach
  - Data-centric security
  - Enterprise information security architecture
  - Identify-based security
  - Information infrastructure
  - Information security audit
  - Information security indicators
  - Information security management
  - Information security standards
  - Information technology
  - Information technology security audit
  - IT risk
  - ITIL security management
  - Gordon-Loeb model for cyber security investments
- Kill chain
  - List of computer security certifications
  - Mobile security
  - Network Security Services
  - Privacy engineering
  - Privacy software
  - Privacy-enhancing technologies
  - Security bug
  - Security convergence
  - Security information management
  - Security level management
  - Security of Information Act
  - Security service (telecommunication)
  - Single sign-on
  - Verification and validation

References

1. <sup>↑</sup> Curry, Michael; Marshall, Byron; Crossier, Robert E.; Correia, John (2018-04-25). "InfoSec Process Action Model (PAM): Systematically Addressing Individual Security Behavior" *in*: ACM SIGSIS Database: The DATABASE for Advances in Information Systems. **49** (5): 40–45. doi:10.1145/3210550.3210558 *in*. ISBN 0005-0033 *in*. SCID 14003080 *in*.

2. <sup>↑</sup> Joshi, Chanchale, Singh, Umesh Kumar (August 2017). "Information security risk management framework – A step towards mitigating security risks in university network" *in*. *Journal of Information Security and Applications*. **35**: 128–137. doi:10.1016/j.jsa.2017.06.005 *in*. ISSN 2214-2120 *in*.

3. <sup>↑</sup> Flöschel, Martin (14 December 2018). "An Introduction to Information risk" *in*. The National Archives. Retrieved 23 February 2022.

4. <sup>↑</sup> "SANS Institute: Information Security Resources" *in*. www.sans.org. Retrieved 2020-10-31 (link not retrieved).

5. <sup>↑</sup> Daniel, Kent; Timan, Sheridan (August 2008). "Market Reactions to Tangible and Intangible Information" *in*. *The Journal of Finance*. **61** (4): 1805–1842. doi:10.1111/j.1540-6261.2006.00834.x *in*. ISBN 0-471-01117-1.

6. <sup>↑</sup> Fink, Karsten (2004). *Knowledge Potential Measurement and Uncertainty*. Deutscher Universitätsverlag. ISBN 978-3-032-91240-7. OCLC 851734708 *in*.

7. <sup>↑</sup> Kayser, Tobias (2018-04-19). "Security policy" *in*. *The Information Governance Toolkit*. CRC Press. pp. 67–82. doi:10.1201/9781315336488-13 *in*. ISBN 978-1-315-33648-8. retrieved 2021-05-28

8. <sup>↑</sup> Dancig, Richard (1995). "The big three: Our greatest security risks and how to address them" (Document). DTIC ADA21883 *in*. {{cite document}}: Cite document requires |url= (help). 1995.

9. <sup>↑</sup> Lyu, M.-R.; Lau, L.-K.Y. (2000). "Firewall security: Policies, testing and performance evaluation" *in*. *Proceedings 26th Annual International Computer Software and Applications Conference*. COMPSAC2000. IEEE Comput. Soc. pp. 116–121. doi:10.1109/compos.2000.894700 *in*. ISBN 0-7895-6782-1. SCID 11202223 *in*.

10. <sup>↑</sup> "How the Lack of Data Standardization Impedes Data-Driven Healthcare" *in*. *Data-Driven Healthcare*. Hoboken, NJ, US: John Wiley & Sons, Inc. p. 29. 2016-10-17. doi:10.1002/9781119205912.ch3 *in*. ISBN 978-1-119-20591-2. retrieved 2021-05-28

11. <sup>↑</sup> Lent, Tom; Walsh, Bill (2009). "Rethinking Open: Building Standards for Comprehensive Continuous Improvement" *in*. *Common Ground, Consensus Building and Continual Improvement: International Standards and Sustainable Building*. West Conshohocken, PA: ASTM International. pp. 1–1. doi:10.1520/bst-47116x *in*. ISBN 978-0-001-43071-8. retrieved 2021-05-28

12. <sup>↑</sup> <sup>↑</sup> Cherdantseva, Y. and Hilton, J. "Information Security and Information Assurance: The Discussion about the Meaning, Scope and Goals". In: *Organizational, Legal, and Technological Dimensions of Information System*

200. <sup>↑</sup> "Authorization And Approval Program" *in*. *Internal Controls Policies and Procedures*. Hoboken, NJ, US: John Wiley & Sons, Inc. pp. 59–72. 2018-10-22. doi:10.1002/9781119205904.ch10 *in*. ISBN 978-1-119-20590-4. retrieved 2021-05-21

201. <sup>↑</sup> "What responses under what conditions?" *in*. *Local Policies and the European Social Fund*. Policy Press. pp. 91–102. 2019-10-02. doi:10.2307/1060671 *in*. ISBN 978-1-4473-4052-4. SCID 24143870 *in*. retrieved 2021-05-01

202. <sup>↑</sup> Cheng, Liang; Zhang, Yang; Han, Zhihui (June 2015). "Quantitatively Measure Access Control Mechanisms across Different Operating Systems" *in*. *2015 IEEE 7th International Conference on Software Security and Reliability*. IEEE. pp. 50–59. doi:10.1109/ikern.2015.12 *in*. ISBN 978-1-4799-2409-8. SCID 1526134 *in*.

203. <sup>↑</sup> "P. Papay, Sharon H. (2000). "discretionary access control". *Computer Science and Communications Dictionary*, p. 426. doi:10.1007/1-4020-0813-5\_522 *in*. ISBN 978-0-7023-8425-0

204. <sup>↑</sup> "Intrinsic Security of the Quantum Transporter SAQC1 Homomorph Function Independence of Each Other" *in*. *arXiv*. doi:10.1021/b050067h.x001 *in*. Retrieved 2021-05-01.

205. <sup>↑</sup> Ellis Ormrod, Jeanne (2012). *Essentials of educational psychology : big ideas to guide effective teaching*. Pearson. ISBN 978-0-13-136127-2. OCLC 95385375 *in*.

206. <sup>↑</sup> Belim, S. V.; Bogochenko, N. F.; Kabanov, A. N. (November 2018). "Security Level of Permissions in Role-Based Access Control" *in*. *2018 Dynamics of Systems, Mechanisms and Machines (Dynamics)*. IEEE. pp. 1–5. arXiv:1812.11454 *in*. doi:10.1109/dynamics.2018.8601480 *in*. ISBN 978-1-5358-8841-0. SCID 8718831 *in*.

207. <sup>↑</sup> "Configuring TACACS and Extended TACACS" *in*. *Securing and Controlling Cisco Routers*. Auerbach Publications. 2002-05-15. doi:10.1201/9781420031484.ch11 *in*. ISBN 978-0-8493-1290-8. retrieved 2021-05-01

208. <sup>↑</sup> "Developing Effective Security Policies" *in*. *Risk Analysis and Security Countermeasure Selection*. CRC Press. pp. 261–274. 2009-12-18. doi:10.1201/9781420078718.ch8 *in*. ISBN 978-0-429-24670-2. retrieved 2021-05-01

209. <sup>↑</sup> "The Use of Audit Trails to Monitor Key Networks and Systems Should Remain Part of the Computer Security Material Weakness" *in*. www.ncsc.gov. Retrieved 2017-10-08.

210. <sup>↑</sup> "Using variable access to machine engine what you need to know about b3368" *in*. *Human Rights Documents online*. doi:10.1183/2210-7875\_110-0002-0152 *in*. Retrieved 2021-08-01.

211. <sup>↑</sup> Salazar, Mary K. (January 2005). "Dealing with Uncertain Risks—When to

Business continuity

Laure and regulations

Culture

Sources of standards

See also

References

➤Further reading

External links

Administrator Almeida F. Porcia, I. (eds.). IOI Global Publishing. (2013).

13. <sup>a</sup> ISO/IEC 27000:2018 (E). (2018). Information technology – Security techniques – Information security management systems – Overview and vocabulary. ISO/IEC.

14. <sup>a</sup> Committee on National Security Systems. National Information Assurance Glossary. CNS5 Instruction No. 4008, 28 April 2010.

15. <sup>a</sup> GSA. (2003). Glossary of terms. 2008. Retrieved from <http://www.isaca.org/gknowledge-Central/Documents/Glossary/glossary.pdf>

16. <sup>a</sup> Pipkin, D. (2000). Information security: Protecting the global enterprise. New York: Hewlett-Packard Company.

17. <sup>a</sup> B. McClenos, E. B. Gier, D. (2001). Information security is information risk management. In Proceedings of the 2001 Workshop on New Security Paradigms NBPW '01. (pp. 87 – 104). ACM. doi:10.1145/508171.508187

18. <sup>a</sup> Anderson, J. M. (2003). "Why we need a new definition of information security". *Computers & Security*, 22 (4): 308–315. doi:10.1016/S0167-4048(03)00407-3

19. <sup>a</sup> Varad, H. S. Buff, J. H. P. (2003). "A taxonomy for information security technologies". *Computers & Security*, 22 (4): 299–307. doi:10.1016/S0167-4048(03)00408-1

20. <sup>a</sup> Gold, S. (December 2004). "Threats looming beyond the perimeter". *Information Security Systems Security*, 2 (2): 10–14. doi:10.1080/10593950500091344

21. <sup>a</sup> Parker, Donn B. (January 1993). "A Comprehensive List of Threats To Information". *Information Systems Security*, 2 (2): 10–14. doi:10.1080/10593950500091344

22. <sup>a</sup> Sullivan, John (2016). "The Evolving Threat Environment". *Building a Corporate Culture of Security*. Elsevier. pp. 33–45. doi:10.1016/B978-0-12-802019-7.0004-3

23. <sup>a</sup> Ewe, C. C., Kuan, D. K., Hernandez, R. B. (2018-12-21). "The analysis of methods of determination of functional types of security of the information-telecommunication system from an unauthorized access". *Problems of Information and Management*, 4 (98). doi:10.18772/2073-4781.4.1313

24. <sup>a</sup> Samaras, S.; Cox, D. (2014). "The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security". *Journal of Information System Security*, 19 (2): 21–45. Archived from the original on 2016-06-22. Retrieved 2018-01-26.

25. <sup>a</sup> "Gartner Says Digital Disruptors Are Impacting All Industries, Digital KPIs Are Crucial to Measuring Success". *Gartner*. 2 October 2017. Retrieved 26 January 2018.

26. <sup>a</sup> "Gartner Survey Shows 42 Percent of CEOs Have Begun Digital Business Transformation". *Gartner*. 24 April 2017. Retrieved 28 January 2018.

27. <sup>a</sup> Fone, Darin; Power, Richard (December 2007). "Baseline controls in some vital but often-overlooked areas of your information protection programme". *Computer Fraud & Security*, 2007 (12): 17–20. doi:10.1016/j.cfs.17200701070107

28. <sup>a</sup> "Low-voltage switchgear and controlgear: Device profile for networked industrial devices". *BSI British Standards*. doi:10.3403/bsstd1015

29. <sup>a</sup> Fazio, James; Hagili, Tim; Hoshio, Kazuo; Howells, Thomas; Srisener, Eiden; Young, Jeffrey (November 2018). "Accounting for Firm Heterogeneity within U.S. Industries: Extended Supply-Use Tables and Trade in Value Added using Enterprise and Establishment Level Data". *Cambridge, MA*. doi:10.3386/w25490

30. <sup>a</sup> "Secure estimation subject to cyber stochastic attacks". *Cloud Control Systems: Emerging Methodologies and Applications in Modeling*. Elsevier. 373–404, 2020. doi:10.1016/B978-0-12-810712-2.00021-4

31. <sup>a</sup> Nijmeijer, H. (2003). *Synchronization of mechanical systems*. World Scientific. ISBN 978-981-278-487-0. OCLC 265346186

32. <sup>a</sup> "Chester J. How students use of computers has evolved in recent years". *doi.org*. doi:10.1787/88933277881

33. <sup>a</sup> "Information technology: Security techniques: Competence requirements for information security management systems professionals". *BSI British Standards*. doi:10.3403/bsstd1071

34. <sup>a</sup> "Information Security Qualifications Fast Sheet". *PDF*. *IT Governance*. Archived from the original [PDF](#) on 10 March 2018. Retrieved 10 March 2018.

35. <sup>a</sup> Ma, Ruijing Ray (March 2016). "Flexible Displays Come in Many Forms". *Information Display*, 32 (2): 4–49. doi:10.1002/2057-4966.2016.00083

36. <sup>a</sup> Rahm, Noor-H. (March 2008). *Human Rights and Internal Security in Malaysia: Rhetoric and Reality*. Defense Technical Information Center. OCLC 74288358

37. <sup>a</sup> Kramer, David (2018-06-14). "Nuclear theft and sabotage threats remain high, report warns". *Physic Today*. doi:10.1088/jpt.6.2.20180614art1. ISBN 1845-0996

Apply the Precautionary Principle". *AACHN Journal*, 54 (1): 11–13. doi:10.1177/10597090050040102

212. <sup>a</sup> "We Need to Know More About How the Government Censors its Employees". *Human Rights Documents Online*. doi:10.1183/2210-7075\_104070-20191111

213. <sup>a</sup> "Purdue. Jerry (2004-04-22). "1001 Computer Words You Need to Know". Oxford University Press. doi:10.1093/acprof:oso/9780161878730.003.0007

214. <sup>a</sup> Easton, William (2021). "Elliptic Curve Cryptography". *Modern Cryptography*. Cham: Springer International Publishing. pp. 245–266. doi:10.1007/978-3-030-83116-4\_119. ISBN 978-3-030-83114-7. S2CID 234109591

215. <sup>a</sup> Faltman, Rebecca (2014-03-01). *From Someone Who Has Been There: Information Sleuthing in Identity*. *Conference 2014 Proceedings (Thess)*. Birkbeck. doi:10.1017/9781107142227

216. <sup>a</sup> Vesta, Jason (2004). "Message Digests, Message Authentication Codes, and Digital Signatures". *Java Cryptography Extensions*. Elsevier. pp. 101–118. doi:10.1016/B978-0-12742751-5/500012-6

217. <sup>a</sup> Bide, D. (March 2018). "Use of RSA Keys with SHA-256 and SHA-512 in the Secure Shell (SSH) Protocol". doi:10.17487/6832

218. <sup>a</sup> Non, Jaewon, Kim, Jeongyeon, Kwon, Owon, Cho, Sunghyun (October 2016). "Secure key exchange scheme for WPA/WPA2-PSK using public key cryptography". *2016 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia)*. IEEE. pp. 1–4. doi:10.1109/icea-2016.7584743

219. <sup>a</sup> Van Buren, Ray F. (May 1990). "How you can use the data encryption standard to encrypt your files and data bases". *ACM SIGSAC Review*, 8 (2): 33–38. doi:10.1145/1012610.101152

220. <sup>a</sup> Bonneau, Joseph (2016). "Why Buy when You Can Rent?". *Financial Cryptography and Data Security, Lecture Notes in Computer Science*. Berlin, Heidelberg: Springer Berlin Heidelberg. vol. 9504. pp. 19–20. doi:10.1007/978-3-662-53287-4\_2

221. <sup>a</sup> Coleman, Heather; Andron, Jeff (2018-08-01). "What GIS Experts and Policy Professionals Need to Know about Using Maxar in Multiojective Planning Processes". *Ocean Solutions, Earth Solutions, Earth Place*. doi:10.17126/9781559483051\_21

222. <sup>a</sup> "P. Lindorff, Peter (2005). "Key Encryption Key". *Encyclopedia of Cryptography and Security*. pp. 326–327. doi:10.1007/s10249-007-2201-7. ISBN 978-3-387-23473-1

223. <sup>a</sup> Qin, Debasis; Banua, Priyayan; Srivastava, P. D.; Jana, Biswasani (2010). "A Cryptosystem for Encryption and Decryption of Long Confidential Messages". *Information Security and Assurance*. Communications in Computer and Information Science, vol. 76. Berlin, Heidelberg: Springer Berlin Heidelberg. pp. 89–98. Bibcode:2010csa.conf..089Q. doi:10.1007/978-3-642-13265-7\_9

224. <sup>a</sup> "Video from SPIE – the International Society for Optics and Photonics". *doi.org*. doi:10.1117/1.2280328.54934932001

225. <sup>a</sup> Valtchaneni, S. R. (2008). *Corporate Management: Governance, and Ethics Best Practices*. John Wiley & Sons. p. 288. ISBN 9781412595933

226. <sup>a</sup> Shon Henry (2003). *All-in-one CISSP Certification Exam Guide* (2nd ed.). Emeryville, California: McGraw-Hill/Osborne. ISBN 978-0-07-222959-8.

227. <sup>a</sup> Boncardo, Robert (2018-06-20). "Jean-Claude Mitrav's Maternal: Nothing Has Taken Place". *Edinburgh University Press*. 1. doi:10.3386/harvard.9781474456353.003.0006

228. <sup>a</sup> "The Importance of Operational Due Diligence". *Heide Fund Operational Due Diligence*. Hoboken, NJ. doi:10.1002/9781119174552.ch2

229. <sup>a</sup> Hall, Gaylord C. (March 1917). "Some Important Diagnostic Points the General Practitioner [sic] Should Know About the Nose". *Southern Medical Journal*, 10 (3): 211. doi:10.1097/00007811-191703000-00007

230. <sup>a</sup> Rens, J. (1996). *Landshappen van IJsser en Peil: een topografisch-antiquarisch onderzoek in het zwaaiende gebied Hoorn en Eldebo-Limburg*. Etnia. ISBN 90-74352-64-2. OCLC 76297414

231. <sup>a</sup> Thomas, Brook (2017-08-22). "Minding Previous Steps Taken". *Oxford Scholarship Online*. doi:10.1093/acprof:oso/9780190456598.003.0002

232. <sup>a</sup> Lindgren, Regina E. (2018). *Risk communication: a handbook for communicating environmental, safety, and health risks*. Wiley. ISBN 978-1-119-49513-1. OCLC 1043892962



38. <sup>a</sup> "Working towards a world with no information risk and security / preventing and preventing workplace computer crime. Routledge. ISBN 978-1-351-92750-0. OCLC 105218207.

39. <sup>a</sup> Stewart, James (2012). *CISAP Study Guide*. Canada: John Wiley & Sons. pp. 255-257. ISBN 978-1-119-01417-3.

40. <sup>a</sup> "2.2. Productivity growth has been trending down in many sectors". *dx.doi.org*. doi:10.1787/734700049750. *Retrieved 2021-05-28*.

41. <sup>a</sup> "Identity Theft: The Newest Digital Attacking Industry Must Take Security". *Issues in Information Systems*. 2007. doi:10.48002/iis\_2007\_287-300. ISBN 1528-7314. *Retrieved 2021-05-28*.

42. <sup>a</sup> Wende-Persson, Anna; Rönneberg, Fredrik (2017). *IT-säkerhet och information - De nya världens säkerhetsrisker och säkerhetsutmaningar*. Umeå universitet. Institutionen för informatik. OCLC 1233859731.

43. <sup>a</sup> Engle, Eric (6 April 2017). "Stone Temple". *Archived from the original on 27 April 2018*. *Retrieved 17 November 2017*. *Cell phones*.

44. <sup>a</sup> Shor, Ruden; Slavicki, Denise P. (2014). "Technology toward the Customers who Mistrusted Employees Scale". *PaycTESTS Dataset*. doi:10.1037/1053-0001. *Retrieved 2021-05-28*.

45. <sup>a</sup> Kichen, Julie Luna (2008). "Trade – Company Information, Company Formations and Property Searches". *Legal Information Management*. 8 (2): 148. doi:10.1017/1472895808000354. ISBN 1472-8958. S2CID 144325193. *Retrieved 2021-05-28*.

46. <sup>a</sup> "Young, Courtney (2018-05-08). "Working with panic attacks". *Help Yourself Towards Mental Health*. Routledge. pp. 200-214. doi:10.4324/9780420475474-32. *Retrieved 2021-05-28*.

47. <sup>a</sup> "Introduction: Inside the Insider Threat". *Insider Threats*. Cornell University Press. pp. 1–9. 2017-12-31. doi:10.7591/9781501708948-003. *Retrieved 2021-05-28*.

48. <sup>a</sup> "Table 7.7: France: Comparison of the profit shares of non-financial corporations and non-financial corporations plus unincorporated enterprises". *dx.doi.org*. doi:10.1787/888933144055. *Retrieved 2021-05-28*.

49. <sup>a</sup> "How Did All Come About?". *The Compliance Business and Its Customers*. Basingstoke: Palgrave Macmillan. 2012. doi:10.1057/9781137211500.0007. ISBN 978-1-137-21150-0. *Retrieved 2021-05-28*.

50. <sup>a</sup> Gordon, Lawrence A.; Loeb, Martin P. (November 2002). "The Economics of Information Security Investment". *ACM Transactions on Information and System Security*. 5 (4): 436–457. doi:10.1145/581271.581274. S2CID 15007867.

51. <sup>a</sup> Cho Kim, Byung; Khana, Lars; James, Tabitha (July 2011). "Individual Trust and Consumer Risk Perception". *Journal of Information Privacy and Security*. 7 (3): 3–22. doi:10.1080/15558648.2011.10585919. *Retrieved 2021-05-28*. S2CID 144403951.

52. <sup>a</sup> Stewart, James (2012). *CISAP Certified Information Systems Security Professional Study Guide 2nd Edition*. Canada: John Wiley & Sons, Inc. pp. 255-257. ISBN 978-1-119-01417-3.

53. <sup>a</sup> Silect, John (March 1994). "The cost-benefit of outsourcing: assessing the true cost of your outsourcing strategy". *European Journal of Purchasing & Supply Management*. 1 (1): 45–47. doi:10.1016/0959-7012(94)90042-0. ISBN 0959-7012.

54. <sup>a</sup> "2.1. Despite strong growth, Austria has lost some ground since the early 1990s". *dx.doi.org*. doi:10.1787/848172085002. *Retrieved 2021-05-28*.

55. <sup>a</sup> "Introduction: Caesar Is Dead: Long Live Caesar!". *Julius Caesar's Self-Created Image and Its Creative Afterlife*. Bloomington Academic. 2018. doi:10.5040/9781474245784.0005. *Retrieved 2021-05-28*. ISBN 978-1-4742-4578-4.

56. <sup>a</sup> Suetonius Tranquillus, Gaius (2008). *Lives of the Caesars (Oxford World's Classics)*. New York: Oxford University Press. p. 28. ISBN 978-0-19-537559-3.

57. <sup>a</sup> Singh, Simon (2000). *The Code Book: Ancho*. pp. 289–290. *Retrieved 2021-05-28*. ISBN 978-0-385-49324-6.

58. <sup>a</sup> Tan, Heng Chuan (2017). *Towards trusted and secure communications in a vehicular environment* (Thesis). Nanjang Technological University. doi:10.32031/1028972758.

59. <sup>a</sup> Johnson, John (1997). *The Evolution of British Sign: 1653-1939*. Her Majesty's Stationery Office. ASIN B000YX10X2.

60. <sup>a</sup> Wilson, Matthew (14 September 2018). "Were Banks Special? Contrasting Viewpoints in Mid-Nineteenth Century Britain". doi:10.2139/ssrn.3246010. S2CID 159005130.

61. <sup>a</sup> Ruppert, K. (2011). "Official Secrets Act (1889, New 1911, Amended 1920, 1939, 1989)". *dx.doi.org*. doi:10.1787/848172085002. *Retrieved 2021-05-28*.

62. <sup>a</sup> "2. The Clayton Act: A consideration of section 2, defining unlawful price discrimination". *The Federal Anti-Trust Law*. Columbia University Press. pp. 18–28, 1900-12-31. doi:10.7554/9780545240033. ISBN 978-0-231-10000-8.

232. <sup>a</sup> Jensen, Eric Tabor (2020-12-03). "Due Diligence in Cyber Activities". *Due Diligence in the International Legal Order*. Oxford University Press. pp. 252–270. doi:10.1093/acprof:oso/9780198899603.003.0016. ISBN 978-0-19-889960-0. *Retrieved 2021-05-05*.

234. <sup>a</sup> "The Duty of Care Risk Analysis Standard". *DoDRA*. Archived from the original on 2018-08-14. *Retrieved 2018-08-15*.

235. <sup>a</sup> Sutton, Adam; Cranney, Adrian; Wiles, Rod (2005). "Evaluating crime prevention". *Crime Prevention*. Cambridge: Cambridge University Press. pp. 70–90. doi:10.1017/9780521850401.0001. ISBN 978-0-511-80400-1. *Retrieved 2021-05-05*.

236. <sup>a</sup> Check, Erika (2004-06-15). "FDA considers antidepressant risks for kids". *Nature*. doi:10.1038/news040913-15. *Retrieved 2021-05-05*.

237. <sup>a</sup> Auckland, Cressida (2017-06-18). "Protecting me from my Directive: Ensuring appropriate safeguards for Academic Directives in Denmark". *Medical Law Review*. 26 (1): 73–97. doi:10.1093/medlaw/mwx037. ISBN 0867-0742. *PMID 28681894*.

238. <sup>a</sup> Takash, George S. (2019). "Preparing for Breach Litigation". *Data Breach Preparation and Response*. Elsevier. pp. 217–230. doi:10.1016/B978-0-12-803451-4.00005-5. *Retrieved 2021-05-05*. ISBN 978-0-12-803451-4.

239. <sup>a</sup> Westry, J.R.; Allen, J.H. (August 2007). "Governance for Enterprise Security (GES) Implementation Guide" (PDF). Software Engineering Institute. *Retrieved 25 January 2018*.

240. <sup>a</sup> Fowler, Kevine (2018). "Developing a Computer Security Incident Response Plan". *Data Breach Preparation and Response*. Elsevier. pp. 49–77. doi:10.1016/B978-0-12-803451-4.00002-4. ISBN 978-0-12-803451-4. *Retrieved 2021-05-05*.

241. <sup>a</sup> Blochl, Fabio (2018). "Proving Limits of State Data Breach Notification Laws: Is a Failure Law the Most Adequate Solution?". *Journal of Information Policy*. 8: 184–208. doi:10.1023/j:info.8.2018.0164. JSTOR 10.3326/jinfo.8.2018.0164.

242. <sup>a</sup> "Understanding Plan for Every Part". *Turbo Flow, Productivity Press*. pp. 21–26, 2017-07-27. doi:10.1021/b978-0-12-810339-8. *Retrieved 2021-05-05*.

243. <sup>a</sup> P P Wills, Leonard (27 February 2016). "A Brief Guide to Handling a Cyber Incident". *American Bar Association*.

244. <sup>a</sup> Johnson, Leggett R. (2014). "Part 1: Incident Response Team". *Computer Incident Response and Forensics Team Management*. Elsevier. pp. 17–19. doi:10.1016/B978-1-98749-698-5.00008-4. *Retrieved 2021-05-05*. ISBN 978-1-98749-698-5.

245. <sup>a</sup> "Computer Incident Response and Forensics Team Management". *Network Security*. 2014 (2): 4. February 2014. doi:10.1016/j:ns.4588(14)70018-2. ISBN 1385-4895.

246. <sup>a</sup> "Cybersecurity Threat Landscape and Future Trends". *Cybersecurity Routledge*. pp. 304–343, 2015-04-16. doi:10.1201/b18335-12. *Retrieved 2021-05-05*. ISBN 978-0-429-26038-4.

247. <sup>a</sup> "Information Technology Security techniques: Information security incident management". *BSI British Standards*. doi:10.3403/30268379. *Retrieved 2021-05-05*.

248. <sup>a</sup> "Investigation of a Flow Shop Clogging Incident: A Precautionary Note on the Use of TQM in Commercial-Scale Continuous Process". *dx.doi.org*. doi:10.1021/bk-1992-0005. *Retrieved 2021-05-05*.

249. <sup>a</sup> Turner, Tim (2011-08-07). "Our Beginning: Team Members Who Began the Success Story". *One Team on All Levels*. Productivity Press. pp. 6–38. doi:10.4324/9781480500228-2. *Retrieved 2021-05-05*. ISBN 978-0-429-25114-0.

250. <sup>a</sup> Erlanger, Leon (2002). *Defensive Strategies*. PC Magazine. p. 70.

251. <sup>a</sup> "Belgium's main street: The event took place in Brussels". *Radical Street Performance*. Routledge. pp. 81–83, 2013-11-05. doi:10.4324/9781315005140-28. *Retrieved 2021-05-05*. ISBN 978-1-315-00514-0.

252. <sup>a</sup> "Why Choice Matters So Much and What Can Be Done to Preserve It: The Manipulation of Choice". *Palgrave Macmillan*. 2013. doi:10.1057/978113713577.021017. ISBN 978-1-137-31357-3. *Retrieved 2021-05-05*.

253. <sup>a</sup> P P "Computer Security Incident Handling Guide" (PDF). Nist.gov. 2012.

254. <sup>a</sup> Bergarini, Emilia; Sengbom, Joachim; Vileth, Maria; Bommarco, Riccardo (4 April 2016). "Table 23: Results from threat-mind modes where non-significant [sic] parameters have not been removed". *Peas*. 4: e1987. doi:10.7717/peer.1987sup-5q.

255. <sup>a</sup> Pembid, David (2005). "Selecting, Copying, Moving and Deleting Files and Directories". *ECOL: Module 2: Using the Computer and Managing Files*. London: Springer London. pp. 88–94. doi:10.1007/978-1-4471-0491-9\_8. *Retrieved 2021-05-05*. ISBN 978-1-85233-443-7.

256. <sup>a</sup> Duma, Omer (2018). *ASP.NET Core 2 Fundamentals: Build Cross-Platform Apps and Dynamic Web Services with The Serverless Web Application Framework*. Pack Publishing Ltd. ISBN 978-1-75903-355-2. *Retrieved 2021-05-05*.

- Business continuity
- Laws and regulations
- Culture
- Sources of standards
- See also
- References
- Further reading
- External links

88377-0, retrieved 2021-08-29.

63. ↑ Maai, Luenda. Day 32 December 2008). "Official Secrecy" (PDF). *Federation of American Scientists*.
64. ↑ "The Official Secrecy Act 1950 which replaced section 2 of the 1911 Act of Espionage and Secrecy (Routledge Revivals). Routledge. pp. 287–292, 2019-06-16. doi:10.4324/9781315425191-17. ISBN 978-1-315-84651-6. retrieved 2021-05-29
65. ↑ "Official Secrecy Act: what it covers, when it has been used, questioned" *The Indian Express*. 2019-02-08. Retrieved 2020-08-07.
66. ↑ Singh, Gajendra (November 2015). "'Breaking the Chains with Which We were Bound": The Interrogation Chamber, the Indian National Army and the Negation of Military Identities, 1941–1947" *. *Bala Digital Library of World War II*. doi:10.1163/2360-3196\_0000\_00000040211462\_010-07. Retrieved 2021-05-28.*
67. ↑ Dunanson, Dennis (June 1982). "The scramble to unscramble French industry" *Aspen Affairs*. 13 (2): 181–170. doi:10.1080/0308678208730070707. ISBN 0308-4374-X.
68. ↑ Whelan et al. 2017, pp. 3.
69. ↑ "Allied Power: Mobilizing Hydro-Electricity During Canada's Second World War" *Alfred Power: University of Toronto Press*. pp. 1–2, 2016-12-31. doi:10.3138/978144267117-003-07. ISBN 978-1-4426-1711-7. retrieved 2021-05-29
70. ↑ Guthrie, Joseph T. (2011-05-15). "Officers and Enlisted Men" *. *Soldiers in the Army of Vietnam*. Virginia: University of North Carolina Press. pp. 83–86. doi:10.5149/9780807877869\_guthrie-11-07. ISBN 978-0-8078-3462-3. retrieved 2021-05-28*
71. ↑ "A Slog-Moratorium". N. (2011). *Engine: The Battle for the Code*. Orion. p. 676. ISBN 9781782212306.
72. ↑ Whelan et al. 2017, pp. 4–6.
73. ↑ "Twentieth-Century Modern for Twentieth-Century Communicator" *. *Thomas Martin: The Lutesworn Press*. pp. 160–184, 2013-04-26. doi:10.2307/4016428.13-07. ISBN 978-0-7188-4009-3. retrieved 2021-05-29*
74. ↑ Murphy, Richard C. (2009-09-01). "Building more powerful less expensive supercomputers using Processing-In-Memory (PIM) LDRD final report" . doi:10.2172/969368-07.
75. ↑ "A Brief History of the Internet" . *www.usgob.gov*. Retrieved 2020-03-07.
76. ↑ "Walking through the View of Delt - on Internet" *. *Computers & Graphics*. 25 (5): 927–October 2001. doi:10.1016/S0097-8493(01)00140-2-07. ISBN 0097-8493-07.*
77. ↑ Delavida, L. (2007). "Chapter 24: A History of Internet Security". In de Leeuw, K.M.M.; Bergsma, J. (eds.). *The History of Information Security: A Comprehensive Handbook*§. Elsevier. pp. 581-615-704. ISBN 9780305059599.
78. ↑ Parrin, Chad (30 June 2008). "The CIA Trial" . Retrieved 31 May 2012. doi:10.2172/969368-07.
79. ↑ Sandhu, Ravi; Jagota, Sushil (2000-10-20). "Relational Database Security" *. *Information Security Management Handbook, Four Volume Set*. Academic Publications. doi:10.1016/B9780323243248.ch126-07. ISBN 978-0-346-1068-3. retrieved 2021-05-29*
80. ↑ "Stoneburner, G.; Hayden, C.; Feringa, A. (2004). "Engineering Principles for Information Technology Security" (PDF). *cert.nist.gov*. doi:10.6028/NIST.SP.800-210-01-07. Archived from the original (PDF) on 2011-08-16. Retrieved 2011-08-28.
81. ↑ "A. J. Neumann, N. Stotland and R. D. Webb (1977). "Post-processing audit tools and techniques" (PDF). US Department of Commerce, National Bureau of Standards. pp. 11-3–11-4.
82. ↑ "veed.org" (PDF). Archived from the original (PDF) on May 16, 2011. Retrieved 2014-01-17.
83. ↑ "USDP (Diversity-Assessed system Security Principles): A trip to atlanta" *. *Computers & Security*. 13 (5): 417–January 1995. doi:10.1016/0167-4048(95)00250-7-07. ISBN 0167-4048-07.*
84. ↑ Stake, Rob. "ICSI Blog" .
85. ↑ Azevedo, Vitoria. "Open Information Security Maturity Model" . Retrieved 12 February 2017.
86. ↑ "George Cybenko - George Cybenko's Personal Home Page" (PDF). Archived from the original (PDF) on 2016-05-29. Retrieved 2016-01-05.
87. ↑ Hughes, Jeff; Cybenko, George (21 June 2016). "Quantitative Metrics and Risk Assessment: The Three Tenets Model of Cybersecurity" *. *Technology/Innovation Management Review*. 3 (3). [CHART] . *continuum.net*.*
88. ↑ Beckers, K. (2018). *Pattern and Security Requirements: Engineering-based Establishment of Security Standards* . Springer. p. 100. ISBN 9783319789543.
89. ↑ Fainberg, Stephen E.; Slavovick, Aleksandra B. (2011). "Data Privacy and Confidentiality". *International Encyclopedia of Statistical Science*. pp. 342–344. doi:10.1007/978-3-642-24888-9\_307-07. ISBN 978-3-642-24888-9.

88377-0, retrieved 2021-08-29.

257. ↑ "Do the Students Understand What They Are Learning?" . *Thinkin' about Your Teaching*. Routledge. pp. 36–40, 2005-02-25. doi:10.4324/978020316907-8-07. ISBN 978-0-203-16907-7. retrieved 2021-05-29
258. ↑ "Where Are Films Restored, Where Do They Come From and Who Restores Them?" . *Film Restoration*. Palgrave Macmillan. 2013. doi:10.1007/9781137287274\_00000107. ISBN 978-1-137-32872-4. retrieved 2021-05-29
259. ↑ Liao, Qi; Li, Zhen; Striegel, Aaron (2011-01-24). "Could firewall rules be public - a game theoretical perspective" *. *Security and Communication Networks*. 5 (2): 187-210. doi:10.1002/sec.337-07. ISBN 1638-9144-07.*
260. ↑ Boeckman, Philip; Greenwald, David J.; Von Bismarck, Nilsur (2013). *Tweeth annual institute on securities regulation in Europe - overcoming deal-making challenges in the current markets*. Practising Law Institute. ISBN 978-1-4024-1933-4. OCLC 123614232-07.
261. ↑ "Figure 1.6. Spending of social security has been growing, while self-financing has been falling" . *di.doi.org*. doi:10.1787/888932459242-07. Retrieved 2021-05-29
262. ↑ "Information Governance: The Crucial First Step" . *Safeguarding Critical E-Document*. Hoboken, NJ, US: John Wiley & Sons, Inc.. pp. 13–24, 2015-06-16. doi:10.1002/9781118204909.ch2-07. ISBN 978-1-119-20490-9. retrieved 2021-05-29
263. ↑ He, Ying (December 1, 2017). "Challenges of Information Security Incident Learning: An Industrial Case Study in a Chinese Healthcare Organization" (PDF). *Informatics for Health and Social Care*. 43 (4): 394–398. doi:10.1080/13581817.2016.1255620-07. PMID 26868160-07. S2CID 20199240-07.
264. ↑ Kamphorst, Roberts R. (1986). "Formal specification of information systems requirements" *. *Information Processing & Management*. 21 (3): 401-414. doi:10.1016/0306-4573(85)90058-07-07. ISBN 0306-4573-07.*
265. ↑ Jenett, H.A. (1998). "Assessment of ecotoxicological risks of element loading from pulp and paper mills - a 3-D OCLC 005474251-07.
266. ↑ "Desktop Computers, Software" . *Practical Pathology Informatics*. New York: Springer-Verlag. pp. 51–82, 2006. doi:10.1007/978-3-540-864-3-07. ISBN 3-540-86430-7-07. retrieved 2021-05-29
267. ↑ Wilby, R.L.; Orr, H.G.; Helger, M.; Fornes, D.; Blackmore, M. (December 2005). "Risks posed by climate change to the delivery of Water Framework Directive objectives in the UK" *. *Environment International*. 32 (3): 1043–1055. doi:10.1016/j.envint.2008.06.017-07. ISBN 0169-4129-07. PMID 18657260-07.*
268. ↑ Campbell, T. (2016). "Chapter 14: Secure Systems Development" . *Practical Information Security Management: A Complete Guide to Planning and Implementation*. apress. p. 218. ISBN 978-1-642-10586-07.
269. ↑ Koppelman, Kari L. (2011). *Understanding human differences : multicultural education for a diverse America*. Pearson|Allyn & Bacon. OCLC 1245810910-07.
270. ↑ "POST-PRODUCTION" *. *Simple Scene, Sensational Shot*. Routledge. pp. 128–147, 2011-04-12. doi:10.4324/9780240821351-07. ISBN 978-0-340-32136-1. retrieved 2021-05-29*
271. ↑ Kumar, Bray; Kama, Tara; Kumar, Vinita; Ravi, Binod Kumar. *Deepends* (2016). "Quintary: How It Can Prove Fatal Even in Apparently Simple Cases: A Case Report" *. *Madras-Legal Updates*. 16 (2): 75. doi:10.5958/0974-1333.2016.00053-07. ISSN 0971-720X-07.*
272. ↑ Flint, Sally (2010-02-22). "Shared roles and responsibilities in flood risk management" *. *Journal of Flood Risk Management*. 12 (1): e12508. doi:10.1111/j.1365-3113.07.02508-07. ISBN 1753-318X-07. S2CID 13378688-07.*
273. ↑ United States. Department of Energy. Office of Inspector General. Office of Scientific and Technical Information (2009). *Audit Report: Fire Protection Deficiencies at Los Alamos National Laboratory*. United States. Dept. of Energy. OCLC 737238180-07.
274. ↑ "Tom, Elaine Q. January 1992). "Managing change in libraries and information services: A systems approach" *. *Information Processing & Management*. 28 (2): 231–282. doi:10.1016/0306-4573(92)90052-2-07. ISBN 0306-4573-07.*
275. ↑ "Abolitionist, Paul (2003). "The Change Management Process Implemented at IDS Sohar" . *Business Process Change Management*. Berlin, Heidelberg: Springer Berlin Heidelberg. pp. 15–22. doi:10.1007/978-3-642-24703-2\_07. ISBN 978-3-642-24703-2. retrieved 2021-05-29
276. ↑ Dawson, Chris (2002-07-01). *Leading Culture Change* . doi:10.1519/9780280474873-07. ISBN 9780280474873. S2CID 242348822-07.
277. ↑ McCormick, Douglas P. (22 March 2016). *Family Inc. - using business principles to maximize your family's wealth*. John Wiley & Sons. ISBN 978-1-119-21679-7. OCLC 845552737-07.
278. ↑ Schuler, Raher (August 1995). "Some properties of sets tractable under every polynomial-time computable distribution" *. *Information Processing Letters*. 55 (4): 173–184. doi:10.1016/S0020-0198(95)00158-0-07. ISBN 0020-0198-07.*

88377-0, retrieved 2021-08-29.

- Business continuity
- Laws and regulations
- Culture
- Sources of standards
- See also
- References
- Further reading
- External links

88377-0, retrieved 2021-08-29.

63. ↑ Maai, Luenda. Day 32 December 2008). "Official Secrecy" (PDF). *Federation of American Scientists*.
64. ↑ "The Official Secrecy Act 1950 which replaced section 2 of the 1911 Act of Espionage and Secrecy (Routledge Revivals). Routledge. pp. 287–292, 2019-06-16. doi:10.4324/9781315425191-17. ISBN 978-1-315-84651-6. retrieved 2021-05-29
65. ↑ "Official Secrecy Act: what it covers, when it has been used, questioned" *The Indian Express*. 2019-02-08. Retrieved 2020-08-07.
66. ↑ Singh, Gajendra (November 2015). "'Breaking the Chains with Which We were Bound": The Interrogation Chamber, the Indian National Army and the Negation of Military Identities, 1941–1947" *. *Bala Digital Library of World War II*. doi:10.1163/2360-3196\_0000\_00000040211462\_010-07. Retrieved 2021-05-28.*
67. ↑ Dunanson, Dennis (June 1982). "The scramble to unscramble French industry" *Aspen Affairs*. 13 (2): 181–170. doi:10.1080/0308678208730070707. ISBN 0308-4374-X.
68. ↑ Whelan et al. 2017, pp. 3.
69. ↑ "Allied Power: Mobilizing Hydro-Electricity During Canada's Second World War" *Alfred Power: University of Toronto Press*. pp. 1–2, 2016-12-31. doi:10.3138/978144267117-003-07. ISBN 978-1-4426-1711-7. retrieved 2021-05-29
70. ↑ Guthrie, Joseph T. (2011-05-15). "Officers and Enlisted Men" *. *Soldiers in the Army of Vietnam*. Virginia: University of North Carolina Press. pp. 83–86. doi:10.5149/9780807877869\_guthrie-11-07. ISBN 978-0-8078-3462-3. retrieved 2021-05-28*
71. ↑ "A Slog-Moratorium". N. (2011). *Engine: The Battle for the Code*. Orion. p. 676. ISBN 9781782212306.
72. ↑ Whelan et al. 2017, pp. 4–6.
73. ↑ "Twentieth-Century Modern for Twentieth-Century Communicator" *. *Thomas Martin: The Lutesworn Press*. pp. 160–184, 2013-04-26. doi:10.2307/4016428.13-07. ISBN 978-0-7188-4009-3. retrieved 2021-05-29*
74. ↑ Murphy, Richard C. (2009-09-01). "Building more powerful less expensive supercomputers using Processing-In-Memory (PIM) LDRD final report" . doi:10.2172/969368-07.
75. ↑ "A Brief History of the Internet" . *www.usgob.gov*. Retrieved 2020-03-07.
76. ↑ "Walking through the View of Delt - on Internet" *. *Computers & Graphics*. 25 (5): 927–October 2001. doi:10.1016/S0097-8493(01)00140-2-07. ISBN 0097-8493-07.*
77. ↑ Delavida, L. (2007). "Chapter 24: A History of Internet Security". In de Leeuw, K.M.M.; Bergsma, J. (eds.). *The History of Information Security: A Comprehensive Handbook*§. Elsevier. pp. 581-615-704. ISBN 9780305059599.
78. ↑ Parrin, Chad (30 June 2008). "The CIA Trial" . Retrieved 31 May 2012. doi:10.2172/969368-07.
79. ↑ Sandhu, Ravi; Jagota, Sushil (2000-10-20). "Relational Database Security" *. *Information Security Management Handbook, Four Volume Set*. Academic Publications. doi:10.1016/B9780323243248.ch126-07. ISBN 978-0-346-1068-3. retrieved 2021-05-29*
80. ↑ "Stoneburner, G.; Hayden, C.; Feringa, A. (2004). "Engineering Principles for Information Technology Security" (PDF). *cert.nist.gov*. doi:10.6028/NIST.SP.800-210-01-07. Archived from the original (PDF) on 2011-08-16. Retrieved 2011-08-28.
81. ↑ "A. J. Neumann, N. Stotland and R. D. Webb (1977). "Post-processing audit tools and techniques" (PDF). US Department of Commerce, National Bureau of Standards. pp. 11-3–11-4.
82. ↑ "veed.org" (PDF). Archived from the original (PDF) on May 16, 2011. Retrieved 2014-01-17.
83. ↑ "USDP (Diversity-Assessed system Security Principles): A trip to atlanta" *. *Computers & Security*. 13 (5): 417–January 1995. doi:10.1016/0167-4048(95)00250-7-07. ISBN 0167-4048-07.*
84. ↑ Stake, Rob. "ICSI Blog" .
85. ↑ Azevedo, Vitoria. "Open Information Security Maturity Model" . Retrieved 12 February 2017.
86. ↑ "George Cybenko - George Cybenko's Personal Home Page" (PDF). Archived from the original (PDF) on 2016-05-29. Retrieved 2016-01-05.
87. ↑ Hughes, Jeff; Cybenko, George (21 June 2016). "Quantitative Metrics and Risk Assessment: The Three Tenets Model of Cybersecurity" *. *Technology/Innovation Management Review*. 3 (3). [CHART] . *continuum.net*.*
88. ↑ Beckers, K. (2018). *Pattern and Security Requirements: Engineering-based Establishment of Security Standards* . Springer. p. 100. ISBN 9783319789543.
89. ↑ Fainberg, Stephen E.; Slavovick, Aleksandra B. (2011). "Data Privacy and Confidentiality". *International Encyclopedia of Statistical Science*. pp. 342–344. doi:10.1007/978-3-642-24888-9\_307-07. ISBN 978-3-642-24888-9.

88377-0, retrieved 2021-08-29.

257. ↑ "Do the Students Understand What They Are Learning?" . *Thinkin' about Your Teaching*. Routledge. pp. 36–40, 2005-02-25. doi:10.4324/978020316907-8-07. ISBN 978-0-203-16907-7. retrieved 2021-05-29
258. ↑ "Where Are Films Restored, Where Do They Come From and Who Restores Them?" . *Film Restoration*. Palgrave Macmillan. 2013. doi:10.1007/9781137287274\_00000107. ISBN 978-1-137-32872-4. retrieved 2021-05-29
259. ↑ Liao, Qi; Li, Zhen; Striegel, Aaron (2011-01-24). "Could firewall rules be public - a game theoretical perspective" *. *Security and Communication Networks*. 5 (2): 187-210. doi:10.1002/sec.337-07. ISBN 1638-9144-07.*
260. ↑ Boeckman, Philip; Greenwald, David J.; Von Bismarck, Nilsur (2013). *Tweeth annual institute on securities regulation in Europe - overcoming deal-making challenges in the current markets*. Practising Law Institute. ISBN 978-1-4024-1933-4. OCLC 123614232-07.
261. ↑ "Figure 1.6. Spending of social security has been growing, while self-financing has been falling" . *di.doi.org*. doi:10.1787/888932459242-07. Retrieved 2021-05-29
262. ↑ "Information Governance: The Crucial First Step" . *Safeguarding Critical E-Document*. Hoboken, NJ, US: John Wiley & Sons, Inc.. pp. 13–24, 2015-06-16. doi:10.1002/9781118204909.ch2-07. ISBN 978-1-119-20490-9. retrieved 2021-05-29
263. ↑ He, Ying (December 1, 2017). "Challenges of Information Security Incident Learning: An Industrial Case Study in a Chinese Healthcare Organization" (PDF). *Informatics for Health and Social Care*. 43 (4): 394–398. doi:10.1080/13581817.2016.1255620-07. PMID 26868160-07. S2CID 20199240-07.
264. ↑ Kamphorst, Roberts R. (1986). "Formal specification of information systems requirements" *. *Information Processing & Management*. 21 (3): 401-414. doi:10.1016/0306-4573(85)90058-07-07. ISBN 0306-4573-07.*
265. ↑ Jenett, H.A. (1998). "Assessment of ecotoxicological risks of element loading from pulp and paper mills - a 3-D OCLC 005474251-07.
266. ↑ "Desktop Computers, Software" . *Practical Pathology Informatics*. New York: Springer-Verlag. pp. 51–82, 2006. doi:10.1007/978-3-540-864-3-07. ISBN 3-540-86430-7-07. retrieved 2021-05-29
267. ↑ Wilby, R.L.; Orr, H.G.; Helger, M.; Fornes, D.; Blackmore, M. (December 2005). "Risks posed by climate change to the delivery of Water Framework Directive objectives in the UK" *. *Environment International*. 32 (3): 1043–1055. doi:10.1016/j.envint.2008.06.017-07. ISBN 0169-4129-07. PMID 18657260-07.*
268. ↑ Campbell, T. (2016). "Chapter 14: Secure Systems Development" . *Practical Information Security Management: A Complete Guide to Planning and Implementation*. apress. p. 218. ISBN 978-1-642-10586-07.
269. ↑ Koppelman, Kari L. (2011). *Understanding human differences : multicultural education for a diverse America*. Pearson|Allyn & Bacon. OCLC 1245810910-07.
270. ↑ "POST-PRODUCTION" *. *Simple Scene, Sensational Shot*. Routledge. pp. 128–147, 2011-04-12. doi:10.4324/9780240821351-07. ISBN 978-0-340-32136-1. retrieved 2021-05-29*
271. ↑ Kumar, Bray; Kama, Tara; Kumar, Vinita; Ravi, Binod Kumar. *Deepends* (2016). "Quintary: How It Can Prove Fatal Even in Apparently Simple Cases: A Case Report" *. *Madras-Legal Updates*. 16 (2): 75. doi:10.5958/0974-1333.2016.00053-07. ISSN 0971-720X-07.*
272. ↑ Flint, Sally (2010-02-22). "Shared roles and responsibilities in flood risk management" *. *Journal of Flood Risk Management*. 12 (1): e12508. doi:10.1111/j.1365-3113.07.02508-07. ISBN 1753-318X-07. S2CID 13378688-07.*
273. ↑ United States. Department of Energy. Office of Inspector General. Office of Scientific and Technical Information (2009). *Audit Report: Fire Protection Deficiencies at Los Alamos National Laboratory*. United States. Dept. of Energy. OCLC 737238180-07.
274. ↑ "Tom, Elaine Q. January 1992). "Managing change in libraries and information services: A systems approach" *. *Information Processing & Management*. 28 (2): 231–282. doi:10.1016/0306-4573(92)90052-2-07. ISBN 0306-4573-07.*
275. ↑ "Abolitionist, Paul (2003). "The Change Management Process Implemented at IDS Sohar" . *Business Process Change Management*. Berlin, Heidelberg: Springer Berlin Heidelberg. pp. 15–22. doi:10.1007/978-3-642-24703-2\_07. ISBN 978-3-642-24703-2. retrieved 2021-05-29
276. ↑ Dawson, Chris (2002-07-01). *Leading Culture Change* . doi:10.1519/9780280474873-07. ISBN 9780280474873. S2CID 242348822-07.
277. ↑ McCormick, Douglas P. (22 March 2016). *Family Inc. - using business principles to maximize your family's wealth*. John Wiley & Sons. ISBN 978-1-119-21679-7. OCLC 845552737-07.
278. ↑ Schuler, Raher (August 1995). "Some properties of sets tractable under every polynomial-time computable distribution" *. *Information Processing Letters*. 55 (4): 173–184. doi:10.1016/S0020-0198(95)0015*

92. <sup>a</sup> **BRCP** **Andress, J.** (2014). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice* (1st ed.). Syngress, p. 240. ISBN 9780132050328.

93. <sup>a</sup> **Burke, J.** **Ehren** (2005). "10 Practitioners' Views on Core Concepts of Information Integrity". *International Journal of Accounting Information Systems*. Elsevier. 6 (4): 260–278. doi:10.1016/j.ijaccinf.2005.07.001.<sup>o</sup>

94. <sup>a</sup> **Hopkins, J.** (2000). "Unauthorized Occupation of Land and Unauthorized Construction: Concepts and Types of Tactical Means of Investigation"<sup>o</sup>. *International Humanitarian University Herald: Jurisprudence* (43): 180–184. doi:10.3284/12007-1788.2002.42.4388. ISBN 2301-7480.<sup>o</sup>

95. <sup>a</sup> **Kim, Eun-Chul** (2000-08-21). "Robustness Integrity for Database Design"<sup>o</sup>. *High-Performance Web Databases*. Auerbach Publications. pp. 427–434. doi:10.1201/9781420316603-447. ISBN 978-0-420-11603-1. retrieved 2021-08-28

96. <sup>a</sup> **Payne, V.** (2018). "Model Threats and Breach the Integrity of Information"<sup>o</sup>. *Systems and Technologies* 2 (5): 80–86. doi:10.3389/2521-6843-2018-2-4648. ISBN 2521-6843.<sup>o</sup>

97. <sup>a</sup> **Fan, Lian; Wang, Yanchun; Cheng, Xiang; Li, Jieming; Jin, Shuyuan** (2013-02-26). "Privacy threat malware multi-process collaboration analysis"<sup>o</sup>. *Security and Communication Networks*. 8 (1): 61–67. doi:10.1002/sec.7056. ISBN 953-0-11447-1.

98. <sup>a</sup> "Completeness, Consistency, and Integrity of the Data Model"<sup>o</sup>. *Measuring Data Quality for Ongoing Improvement: MK Series on Business Intelligence*. Elsevier. 2015. pp. e11–e16. doi:10.1016/B978-0-12-397033-6.00030-4.<sup>o</sup>. ISBN 978-0-12-397033-6. Retrieved 2021-08-28

99. <sup>a</sup> "Video from SPIE - the International Society for Optics and Photonics"<sup>o</sup>. *dx.doi.org*. doi:10.1117/12.2208328.5458349132001.<sup>o</sup>. Retrieved 2021-08-28

100. <sup>a</sup> "Communication Skills Used in Information Systems Graduates"<sup>o</sup>. *Issues in Information Systems*. 2006. doi:10.48000/iis\_2006\_311-317.<sup>o</sup>. ISBN 1630-7314.<sup>o</sup>

101. <sup>a</sup> "Outages of electric power supply resulting from cable failures Boston Edison Company system"<sup>o</sup>. 1980-07-21. doi:10.2172/5083190.<sup>o</sup>. OSTI 5083190.<sup>o</sup>. Retrieved 18 January 2022.

102. <sup>a</sup> **Loukas, G.** **Ota, G.** (September 2010) [August 2009]. "Protection Against Denial of Service Attacks: A Survey"<sup>o</sup>. *IC3P*. *Comput. J.* 53 (7): 1000–1037. doi:10.1093/comjnl/btp079.<sup>o</sup>. Archived from the original <sup>o</sup> (PDF) on 2012-03-24. Retrieved 2016-08-28

103. <sup>a</sup> "Be Able To Perform a Critical Activity"<sup>o</sup>. *Defensible Oeas*. 2020-02-02. doi:10.32388/defnsuff. <sup>o</sup>. SCID 24133732.<sup>o</sup>. retrieved 2021-08-28

104. <sup>a</sup> **Ohta, Mak; Fujii, Takes** (May 2011). "Iterative cooperative sensing on shared primary spectrum for improving sensing ability"<sup>o</sup>. 2011 *IEEE International Symposium on Dynamic Spectrum Access Networks (DYSPAN)*. (IEEE. pp. 623–627. doi:10.1109/dyspan.2011.5936387.<sup>o</sup>. ISBN 978-1-4577-0177-1. SCID 18116653.<sup>o</sup>

105. <sup>a</sup> "Information technology Information security Incident management"<sup>o</sup>. *BSI British Standards*. doi:10.3403/35337743.<sup>o</sup>. retrieved 2021-08-29

106. <sup>a</sup> **Blum, Dan** (2000). "Identify and Align Security-Related Roles"<sup>o</sup>. *Rational Cybersecurity for Business*. Berkeley, CA: Apress. pp. 31–40. doi:10.1007/978-1-4842-8602-8\_2.<sup>o</sup>. ISBN 978-1-4842-8601-1. SCID 22052693.<sup>o</sup>. retrieved 2021-08-29

107. <sup>a</sup> **McCarthy, C.** (2008). "Digital Libraries: Security and Preservation Considerations"<sup>o</sup>. In **Bogdal, H.** (ed.). *Handbook of Information Security: Trends, Vulnerabilities, Prevention, Detection, and Management*. Vol. 3. John Wiley & Sons. pp. 46–78. ISBN 9780470091214.

108. <sup>a</sup> "Information technology Open systems interconnection: Security Frameworks for open systems"<sup>o</sup>. *ISO British Standards*. doi:10.3403/01102050.<sup>o</sup>. retrieved 2021-08-29

109. <sup>a</sup> **Christofor, Raf** (2014-01-01). "This could it have been"<sup>o</sup>. *Julio Rondo - O.A. Meta Memory*. Wilhelm Fink Verlag. doi:10.5996/9783948797813\_053.<sup>o</sup>. ISBN 978-3-7195-6767-1. retrieved 2021-08-29

110. <sup>a</sup> **Akita, D.** (May 2021). "Use of the Walnut Digital Signature Algorithm with CBCR Object Signing and Encryption (COSE)"<sup>o</sup>. doi:10.17487/1869221.<sup>o</sup>. SCID 19255927.<sup>o</sup>. Retrieved 18 January 2022.

111. <sup>a</sup> **Le May, I.** (2003). "Structural Integrity in the Petrochemical Industry"<sup>o</sup>. *Comprehensive Structural Integrity*. Elsevier. pp. 126–149. doi:10.1016/B004749-01/0101-67.<sup>o</sup>. ISBN 978-0-08-040740-1. retrieved 2021-08-29

112. <sup>a</sup> **Bodahn, Amos**. *Champagne, Coddies, Crogins*. **Frank Oller**. **Roland** (2017-01-11). "Leading or lagging indicators of risk? The informational content of extra-financial performance scores"<sup>o</sup>. *Journal of Asset Management*. 18 (6): 347–370. doi:10.1057/s41260-016-0026-x.<sup>o</sup>. ISBN 1470-6272.<sup>o</sup>. SCID 19748590.<sup>o</sup>

113. <sup>a</sup> **Reynolds, E. H** (1968-07-22). "Tobacco has potential to cause harm"<sup>o</sup>. *BMJ*. 3 (61) (666): 287. doi:10.1136/bmj.311.6666.287.<sup>o</sup>. ISBN 0859-6138.<sup>o</sup>. PMC 2560266.<sup>o</sup>. PMID 7553870.<sup>o</sup>

114. <sup>a</sup> **Randal, Alan** (2011). "Harm, risk, and threat"<sup>o</sup>. *Risk and Precaution, Precaution: Precaution: Precaution: Precaution*. pp. 84–85.

115. <sup>a</sup> **Phelps, G. A.** *Change in information systems into generally not not, more than one client"<sup>o</sup> (Bios). dx.doi.org*. doi:10.1787/889335818104.<sup>o</sup>. Retrieved 2021-08-28

116. <sup>a</sup> "Multi-user file server for DOS LANs"<sup>o</sup>. *Computer Communications*. 18 (3): 183. June 1987. doi:10.1016/0140-3648(87)90053-7.<sup>o</sup>. ISBN 0-140-30641-4.

117. <sup>a</sup> "Defining Organizational Change"<sup>o</sup>. *Organizational Change*. Oxford, UK: Wiley-Blackwell. pp. 21–51. 2011-04-18. doi:10.1002/978144430372.ch11.<sup>o</sup>. ISBN 978-14443-0372-2. retrieved 2021-08-28

118. <sup>a</sup> **Kleinert, Matthias**. **Schäfer, August Wilhelm** (2003). "Change Management — Key for Business Process Excellence"<sup>o</sup>. *Business Process Change Management*. Berlin, Heidelberg: Springer Berlin Heidelberg. pp. 1–14. doi:10.1007/978-3-642-04703-0\_1.<sup>o</sup>. ISBN 978-3-642-00532-4. retrieved 2021-08-28

119. <sup>a</sup> **More, Josh**. **Stieber, Anthony J.** **Liu, Chris** (2018). "Tier 2—Advanced Help Desk—Help Desk Supervisor"<sup>o</sup>. *Enabling Info Information Security*. Elsevier. pp. 111–113. doi:10.1016/B978-0-12-400783-8.00026-x.<sup>o</sup>. ISBN 978-0-12-400783-8. retrieved 2021-08-28

120. <sup>a</sup> "An Application of Bayesian Networks in Automated Sorting of Competence Simulation Tasks"<sup>o</sup>. *Automated Sorting of Complex Tasks in Computer-Based Testing*. Routledge. pp. 213–244. 2009-04-04. doi:10.4324/9780415983872-101.<sup>o</sup>. ISBN 978-0-415-08387-2. retrieved 2021-08-28

121. <sup>a</sup> **Kassiraj, Michael J.** (June 1994). "Change, Change, Change"<sup>o</sup>. *Group & Organization Management*. 19 (2): 138–140. doi:10.1177/1059601194162001.<sup>o</sup>. ISBN 1059-6011.<sup>o</sup>. SCID 144198203.<sup>o</sup>

122. <sup>a</sup> **Tejcs, J.** (2000). "Chapter 10: Understanding the Project Change Process"<sup>o</sup>. *Project Scheduling and Cost Control Planning, Monitoring and Controlling the Baseline*. J. Ross Publishing. pp. 187–214. ISBN 9781932189110.

123. <sup>a</sup> "17. Innovation and Change: Can Anyone Do That?"<sup>o</sup>. *Backstage in a Brewery*. University of Texas Press. pp. 67–86. 2017-12-31. doi:10.1515/9780282488036-019.<sup>o</sup>. ISBN 978-0-282-48803-6. retrieved 2021-08-28

124. <sup>a</sup> **Braun, Adam D.** (February 2015). *Promises of a penist: how an ordinary person can create extraordinary change*. **Simon and Schuster**. ISBN 978-1-4587-3093-6. OCLC 902912775.<sup>o</sup>

125. <sup>a</sup> "Describing Within-Person Change Over Time"<sup>o</sup>. *Longitudinal Analysis*. Routledge. pp. 228–268. 2016-01-30. doi:10.4324/9781315744084-144.<sup>o</sup>. ISBN 978-1-315-74408-4. retrieved 2021-08-28

126. <sup>a</sup> **Ingraham, Carolyn**. **San, Patricia W.** (1984). *Legislating bureaucontrol change: the Civil Service Reform Act of 1978*. State University of New York Press. ISBN 0-87395-885-1. OCLC 1030317116.

127. <sup>a</sup> **Wei, J.** (2000-05-04). "Preliminary Change Request for the SWS 1.3 GeV- Compatible Ring"<sup>o</sup>. *CERN DOW*. doi:10.2172/1167263.<sup>o</sup>. OSTI 1157263.<sup>o</sup>. Retrieved 13 January 2022.

128. <sup>a</sup> **Chen, Liang** (May 2011). "Allocation priority management of agricultural water resources based on the theory of virtual water"<sup>o</sup>. 2011 *International Conference on Business Management and Electronic Information*. Vol. 1. IEEE. pp. 644–647. doi:10.1109/bsme.2011.5917018.<sup>o</sup>. ISBN 978-1-61284-108-3. SCID 26137226.<sup>o</sup>

129. <sup>a</sup> "Change risks and best practices in Business Change Management: Unmanaged change not leads to problems for change management"<sup>o</sup>. *Leading and Implementing Business Change Management Routledge*. pp. 32–74. 2015-07-18. doi:10.4324/9780203072657-6.<sup>o</sup>. ISBN 978-0-203-07265-7. retrieved 2021-08-28

130. <sup>a</sup> **Brigg, Steven W.** (2016). *Accounting Best Practices*. Wiley. ISBN 978-1-118-41793-5. OCLC 94692504.<sup>o</sup>

131. <sup>a</sup> "Successful change requires more than change management"<sup>o</sup>. *Human Resource Management International Digest*. 16 (7): 208–10-17. doi:10.1108/hrm-2006-04414gss-0007. ISBN 0881-0734.<sup>o</sup>

132. <sup>a</sup> "Planning for water resources under climate change"<sup>o</sup>. *Spatial Planning and Climate Change*. Routledge. pp. 287–313. 2010-09-13. doi:10.4324/9780203048807-2017. ISBN 978-0-203-04880-7. retrieved 2021-08-28

133. <sup>a</sup> **Rowen, John** (January 1987). "Answering the computer back"<sup>o</sup>. *Management Decision*. 1 (1): 61–64. doi:10.1108/e000707987. ISBN 0025-1717.<sup>o</sup>

134. <sup>a</sup> **Bouas, Margaret R.** **Bouas, Asit K.** (February 1981). "Climate change and food production"<sup>o</sup>. *Agriculture and Environment*. 3 (4): 332. doi:10.1016/0304-1110(81)90050-9.<sup>o</sup>. ISBN 0304-1111.<sup>o</sup>

135. <sup>a</sup> **Wak, Martin H.** (2006). "Backlog". *Computer Science and Communications Dictionary*. p. 98. doi:10.1007/1-4020-0914-8\_1259.<sup>o</sup>. ISBN 978-0-7923-8425-0.

136. <sup>a</sup> "Editorial Advisory and Review Board"<sup>o</sup>. *Business and Sustainability: Concepts, Strategies and Changes*. Critical Studies on Corporate Responsibility, Governance and Sustainability. Emerald Group Publishing Limited. vol. 3. pp. xv-xvii. 2011-12-26. doi:10.1108/0274-9569(2011)0000030001.<sup>o</sup>. ISBN 978-1-78062-436-2. retrieved 2021-08-28

137. <sup>a</sup> "Where a Mirage Has Once Been, Life Must Be"<sup>o</sup>. *New and Selected*.

Business continuity

Laws and regulations

Culture

Sources of standards

See also

References

Further reading

## External links



Business continuity  
Laws and regulations  
Culture  
Sources of standards  
See also  
References  
Further reading  
External links

- ↑ https://high.elsevier.com/locate/jbrs.2021.1000000
- ↑ doi:10.1017/S0057805187458750317, ISBN 978-0-811-47455-7, retrieved 2021-06-29
- ↑ Grama, J. J. (2014). *Legal Issues in Information Security*<sup>[a]</sup>. Jones & Bartlett Learning. p. 550. ISBN 978-1284-919540.
- ↑ Cannon, David L. (2014-03-04). "Audit Process"<sup>[a]</sup>. CISA: Certified Information Systems Auditor Study Guide (Fourth ed.). pp. 136–214. doi:10.1002/9781119416211.ch21. ISBN 9781195059240.
- ↑ "CISA Review Manual 2006: Information Systems Audit and Control Association. 2006. p. 65. ISBN 978-1-403384-15-8.
- ↑ Kaden, Janekow (2013-11-02). "Two-dimensional process modeling (2DPM)"<sup>[a]</sup>. *Business Process Management Journal*. **18** (6): 848–876. doi:10.1108/1463775121128332317. ISBN 1463-775417.
- ↑ "All Countermeasures Have Some Value, But No Countermeasure Is Perfect"<sup>[a]</sup>. *Bayard Fear*. New York: Springer-Verlag. pp. 207–232. 2003. doi:10.1007/s-977-9171-5-4.144. ISBN 0-887-03000-7. retrieved 2021-06-29
- ↑ "Data breaches: Deloitte suffers serious hit while more details emerge about Equifax and Yahoo!"<sup>[a]</sup>. *Computer Fraud & Security*. **2017** (10): 1–3. October 2017. doi:10.1016/j.cfs.2017.07.007. ISBN 1461-2823-1.
- ↑ "Spagnoli, Paolo; Russo A. (2008). "The duality of Information Security Management: fighting against predictable and unpredictable threats"<sup>[a]</sup>. *Journal of Information System Security*. **4** (3): 45–52.
- ↑ "Yusef, Nur Hasbain; "Yusef, Mohd Raduan" (2009-09-04). "Managing HSE Risk in Harsh Environment"<sup>[a]</sup>. *All Days, SPE*. doi:10.2118/122545-ms17.
- ↑ Baker, Wesley (2010). *Sold out: how Obama's downtown business improvement areas have caused and reduced urban space* (Thesis). Carleton University. doi:10.22133/etd-01-2007-01.
- ↑ de Souza, André; Lynch, Anthony (June 2012). "Does Mutual Fund Performance Vary over the Business Cycle?"<sup>[a]</sup>. Cambridge, MA. doi:10.3386/w1813717. SCID 2003034517.
- ↑ Kloutonakis, E.A.; Kokiakakis, S.A. (1999-05-31). *Information systems security: facing the information society of the 21st century*. London: Chapman & Hall, Ltd. ISBN 978-0-412-71910-6.
- ↑ "Newsome, B. (2013). *A Practical Introduction to Security and Risk Management*. SAGE Publications. p. 208. ISBN 9781443324852.
- ↑ "R. Whitman, M.E.; Mattord, H.J. (2018). *Management of Information Security* (9th ed.). Cengage Learning. p. 562. ISBN 9781035551256.
- ↑ "Hardware, Facilities, Activities, and Other Technical Support"<sup>[a]</sup>. *Illustrated Theatre Production Guide*. Routledge. pp. 203–232. 2013-03-20. doi:10.4324/9780080958362-2017. ISBN 978-0-08-095836-2. retrieved 2021-06-29
- ↑ Reason, James (2017-03-02). "Perceptions of Unsafe Acts"<sup>[a]</sup>. *The Human Contribution*. CRC Press. pp. 66–103. doi:10.1201/9781315236125-717. ISBN 978-1-315-23612-6. retrieved 2021-06-29
- ↑ "Information Security Procedures and Standards"<sup>[a]</sup>. *Information Security Policies, Procedures, and Standards*. Boca Raton, FL: Auerbach Publications. pp. 81–82. 2017-03-27. doi:10.1201/9781315372785-817. ISBN 978-1-315-37278-5. retrieved 2021-06-29
- ↑ Zhang, Hailong; Chen, Yu; Sheng, Xianfu; Hong, Lili; Gao, Rulan; Zhuang, Xiaofen (25 June 2020). "Figure S1: Analysis of the prognostic impact of each single signature gene"<sup>[a]</sup>. *Pearl*. **8**: e9437. doi:10.7717/peerj.94371717. SCID 2003034517.
- ↑ Standert, B.; Ethgen, O.; Emerson, R.A. (June 2012). "COA Coas- Effectiveness Analysis - Appropriate for All Situations?"<sup>[a]</sup>. *Value in Health*. **15** (4): A2. doi:10.1016/j.jval.2012.02.0168. ISBN 1508-201417.
- ↑ "GRP vaccines provide cost-effective over-dose protection"<sup>[a]</sup>. *Reinforced Plastics*. **49** (11): 8. November 1999. doi:10.1016/S0034-3817(99)01028-417. ISBN 0034-381717.
- ↑ "Figure 2.3. Relative risk of being a low performer depending on personal circumstances (2012)"<sup>[a]</sup>. *dr.dei.org*. doi:10.1787/88893371741017. Retrieved 2021-06-29
- ↑ Bonebruner, Gary; Ogden, Alice; Feringa, Alexis (2002). "NIST SP 800-30 Risk-Management Guide for Information Technology Systems"<sup>[a]</sup>. doi:10.8028/NIST.SP.800-3017. Retrieved 18 January 2022.
- ↑ "May I Choose? Can I Choose? Oppression and Choice"<sup>[a]</sup>. *A Theory of Freedom*. Palgrave Macmillan. 2012. doi:10.1007/9781137289528\_000717. ISBN 978-1-137-28952-6. retrieved 2021-06-29
- ↑ "Parker, Donn B. (January 1994). "A Guide to Selecting and Implementing Security Controls"<sup>[a]</sup>. *Information Systems Security*. **2** (2): 75–85. doi:10.1080/10589469308803145017. ISSN 1058-946917.
- ↑ Zoccali, Carmine; Mallamaci, Fiorenza; Tripepi, Giovanni (2007-09-26). "Guest Editor: Ravin Agarwal: Cardiovascular Risk Profile Assessment and Medication Control Should Come First"<sup>[a]</sup>. *Zemane's e-Digest*. **20** (5): 495–498. doi:10.1111/j.1925-139x.2007.00317.x17. ISBN 0894-066917. PMID 1789724817. SCID 3328612717.
- ↑ "Guide to the Implementation and Auditing of ISMS Controls based on ISO/IEC 27001:01". London: BSI Group Standards. 2013-11-01. doi:10.3403/97805060829101517. ISBN 978-0-850-62010-6.
- ↑ poema. University of Bolton. ISBN 978-0-144-01474-4. doi:10.2307/10464818617. ISBN 978-1-48117-323-4. retrieved 2021-06-08
- ↑ "Bell, Marvin (1983). "Two, When There Might Have Been Three". *The Antioch Review*. **41** (2): 209. doi:10.2307/481120017. JSTOR 481120017.
- ↑ "You can save alive change"<sup>[a]</sup>. *Human Rights Documents Online*. doi:10.1183/2210-7675\_hrd-0148-201517817. Retrieved 2021-06-05.
- ↑ Mackana, Anthony Tapsia (5 November 2020). "Change is the Law of Life, and Those Who Look only to the past or Present Are Certain to Miss the Future". John F. Kennedy Assessing The Statement with References to Organizations in Zimbabwe Who Have Been Affected by Change". doi:10.2139/ssrn.372870717. SCID 28894940017.
- ↑ Ramchandran, V.V. (ed.). *Privatization in the UK*. ISBN 978-0-409-10070-8. OCLC 10866916417.
- ↑ "More complex rheology must be implemented: Numerical convergence tests must be performed"<sup>[a]</sup>. 2020-09-22. doi:10.1519/jnd-2020-107-u048. SCID 24156197317.
- ↑ "Stone, Edward. *Edward C. Stone Collection*. OCLC 7331021017.
- ↑ "Lantz, B (2002). "Develop Your Improvement Implementation Plan"<sup>[a]</sup>. *Achieve Learning Process Improvement*. Elsevier. pp. 151–171. doi:10.1016/B978-0-12-446994-5.00011-517. ISBN 978-0-12-446994-3. retrieved 2021-06-05
- ↑ Smeets, Peter (2009). *Expeditie sgrppen - ontwerpen ontdekken naar metropoolen/landbouw en duurzaam ontbrekking*. s.n.] ISBN 978-90-5055-915-6. OCLC 441821141017.
- ↑ "Figure 1.3. About 50 percent of the Going for Growth recommendations have been implemented or are in process of implementation"<sup>[a]</sup>. *dr.dei.org*. doi:10.1787/88893333735817. Retrieved 2021-06-05
- ↑ Kelley, John (2019-02-21). "Must Justice Be Done at All Costs?"<sup>[a]</sup>. *Hard Questions*. Oxford University Press. pp. 98–126. doi:10.1093/oxfrhb/9780190916996.003.0005017. ISBN 978-0-19-091699-6. retrieved 2021-06-05
- ↑ "Forrester, Kalle (2014). *Macroeconomic implications of changes in the composition of the labor force*. University of California, Santa Barbara. ISBN 978-1-921-14932-2. OCLC 87418781017.
- ↑ Choudhury, Gagan L.; Rappoport, Stephen G. (October 1981). "Demand assigned multiple access systems using collision type request channels"<sup>[a]</sup>. *ACM SIGCOMM Computer Communication Review*. **11** (4): 126–148. doi:10.1145/1013579.30205017. ISBN 0146-482317.
- ↑ "Crispin, Mark (2013). "Certain Old and Lovely Things, Whose Signified is Abstract, Out of Date". *James Strling and Nostalgia*"<sup>[a]</sup>. *Change over Time*. **3** (1): 118–122. doi:10.1332/act.2013.0001017. ISBN 2153-054817. SCID 14445139317.
- ↑ Alwady, Mansour; Pemberton, Lyn (2018). "What Changes Need to be Made within the L3H3 for Ehealth Systems to be Successfully Implemented?"<sup>[a]</sup>. *Proceedings of the International Conference on Information and Communication Technologies for Aging Well and e-Health*. Scitepress. pp. 71–78. doi:10.5220/000002040071007917. ISBN 978-698-735-1610-9.
- ↑ "Mortimer, John (April 2010). *Paradise postponed*. Penguin Adult. ISBN 978-0-14-104952-6. OCLC 49505836217.
- ↑ "Cobey, Sarah; Lammone, Daniel B.; Grad, Yonatan H.; Lipstich, Marc (2021). "Climate action SARS-CoV-2 evolution should not hold back efforts to expand vaccination"<sup>[a]</sup>. *Nature Reviews Immunology*. **21** (5): 335–336. doi:10.1038/s41577-021-00544-917. PMC 80148938. PMID 3379985617.
- ↑ "Farrington, Michael (2014-12-28). "Processing Data with Map Reduce"<sup>[a]</sup>. *Big Data Made Easy*. Berkeley, CA: Apress. pp. 85–120. doi:10.1007/978-1-4842-0004-0\_17. ISBN 978-1-4842-0005-7. retrieved 2021-06-05
- ↑ "Good study overall, but several procedures need fixing"<sup>[a]</sup> (PDF). 2016: 82-83. doi:10.5194/ham-2015-0201028. Retrieved 18 January 2022.
- ↑ Harrison, Kent; Craft, Walter M.; Hiller, Jack; McCuskey, Michael R. (July 1999). "Peer Review Coordinating Draft: Task Analysis for Conduct Intelligence Planning (Critical Combat Function 1) As Accomplished by a Battalion Task Force" (document). DTIC ADA31384617. [help · add citation · get document · get document requires (pull) link= (help)
- ↑ "tpti.org/" Archived 17 December 10, 2013, at the Wayback Machine
- ↑ "book summary of The Machine Cup Handbook: Implementing ITIL in a Practical and Auditable Steps"<sup>[a]</sup>. *wikisummar.es.org*. Retrieved 2016-05-22.
- ↑ "Bigelow, Mohale (2020-06-23). "Change Control and Change Management"<sup>[a]</sup>. *Implementing Information Security in Healthcare*. HIMSS Publishing. pp. 203–214. doi:10.4242/9781503126264-717. ISBN 978-1-003-12623-4. SCID 22489530717. retrieved 2021-06-05
- ↑ "Business continuity management: Guidance on organization recovery following disruptive incidents"<sup>[a]</sup>. BSI British Standards. doi:10.3403/20150303017. retrieved 2021-06-05
- ↑ "Hoam, Chu Thai (1996). *Development of a computerized aid to integrated land use planning (dalugi) at regional level in irrigated areas - a case study for the Quan Lu Phung Hiep region in the Hoang Delta, Vietnam*. ITC. ISBN 80-6164-120-4. OCLC 50876351517.



20. "Johnson, L. (2019). Security Controls Evaluation, Testing, and Assessment Handbook." Synopsys, B-1780-180126224.
21. "Information Technology Security in 1842: the revised editions of (GPO: 17601 and GPO: 175007). B-1801 Brando, Sanders. doi:10.1201/9781351020281 reviewed 2021-05-29
22. "Administrative Control in Occupational Ergonomics. CRC Press. pp 443-466. 2005-02-28. doi:10.1201/9781351020281.ch23. reviewed 2021-05-29
23. "Chan, J., Demais, E.A., Liu, B. (2018) "How Time of Day Impacts on Security." doi:10.1201/9781351020281. reviewed 18 January 2022
24. "U.S. A. (3-14-57). B-1801
25. "Appendix D of Information Security Framework for Compliance. Autodesk Publications. pp 171-187. 2019-03-22. doi:10.1201/9781351020281.ch17. reviewed 2021-05-29
26. "Firewalls, Intrusion Detection Systems and Vulnerability Assessment: A Topical Collection." In: Network Security. 2022 (9-1). September 2022. doi:10.1016/B978-0-323-98546-1.ch10. reviewed 2021-05-29
27. "Ransome, J., Mura, A. (2013). Core Software Security: Security at the Source." CRC Press. pp 40-41. doi:10.1080/00981968.2013.800668
28. "Volk, Martin H. (2008). "Best practice principles: Computer Science and Communications Dictionary." pp 1031-1032. doi:10.1001/43815-015-10031-1. ISBN 978-0-130733242-0
29. "Emc Astra (September 2018). "The Duties of an Employee's Law. Law. doi:10.1002/9781351020281.ch17. reviewed 2021-05-29
30. "Guide for Information Access Privileges to Health Information." ASTM International. doi:10.1520/00981968-01. reviewed 2021-05-29
31. "Dwyer, Bill (2009-01-21). "Physical Environment." In: Control Techniques, Dries and Control Techniques. Publications of Engineers. doi:10.1002/9781351020281.ch17. reviewed 2021-05-29
32. "Free detection and fire alarm systems." B-1801 Sanders. doi:10.1201/9781351020281. reviewed 2021-05-29
33. "Stevenson, Arnold B. (November 2001). "An important but frequently overlooked procedure." In: JOM. 33 (11-48). Brooks: 2001. JOM. 33(11-48). doi:10.1002/9781351020281.ch17. reviewed 2021-05-29
34. "Many employees pharmacists should be able to benefit." In: The American College of Pharmacy. doi:10.1201/9781351020281. reviewed 2021-05-29
35. "Signification of Duties Control matrix." B-1801 Sanders. Archived from the original on 3 July 2011. doi:10.1201/9781351020281. reviewed 2021-05-29
36. "Residents Must Prove They Are Not in the Line." JAMA. 271 (17). 14108. 1980-05-08. doi:10.1001/jama.271.17.14108. reviewed 2021-05-29
37. "Group Workload Support Systems Aggregating the Insights of Many Through Information Technology." In: Issues in Information Systems. 2008. doi:10.48550/jais.2008.3402. ISBN 978-0-7314-4714-1
38. "INTERDEPENDENCIES OF INFORMATION SYSTEMS." In: Lessons Learned. Critical Information Infrastructure Protection. IT Governance Publishing. pp 34-37. 2017. doi:10.1002/9781351020281.ch17. reviewed 2021-05-29
39. "Managing Network Security." In: Network Parameter Security. Autodesk Publications. pp 11-46. 2009-10-27. doi:10.1002/9781351020281.ch17. reviewed 2021-05-29
40. "Vaccines, A. (2013). Chapter 17: What is Vulnerability Assessment? In: Vaccines. 1 (4). doi:10.1002/9781351020281.ch17. reviewed 2021-05-29
41. "Duke, P. A., Howard, J. P. (2012-09-01). "Processing retail size disparities in distant land places." In: JOM. 33 (11-48). doi:10.1002/9781351020281.ch17. reviewed 2021-05-29
42. "Security Group Control System." In: Network Parameter Security. Autodesk Publications. pp 451-455. doi:10.1002/9781351020281.ch17. reviewed 2021-05-29
43. "Measles Virus." In: The Journal of the Society of Dental Hygiene. 1980. doi:10.1002/9781351020281.ch17. reviewed 2021-05-29
44. "Review of the use of 1021 as a tool for the Study of Dental Hygiene." In: 2021-05-29
45. "Information Security Policy, Procedures, and Standards." American Publications. pp 1-123. doi:10.1002/9781351020281.ch17. reviewed 2021-05-29
46. "Electrical protection rules: Information and requirements for protection rules." In: B-1801 Sanders. doi:10.1201/9781351020281.ch17. reviewed 2021-05-29
47. "Diabene, Joseph D., Reimer, James D., Bue, Michael, Masoud, Giovanni D., Bont, Peter, Baurer, Martin D., Stet, Michael (8 February 2019). "Supplemental information: List of all combined trends in rheumatoid arthritis assigned in MEGA4 with 11 (11-17). In: PLoS. 17 (4072). doi:10.1371/journal.pone.0273966
48. "Kin, Sung-Won (2009-03-21). "Quantitative Analysis of Classification Factors and Classification of Resources of Diversity." In: Journal of Information Management. 17 (1). 85-100. doi:10.1383/jim.2009.1.001

- 169. \* \* P Bayuk, J. (2006). "Chapter 4: Information Classification" in *Aswath: C.W. Bayuk, J.L. Schuch, C. eds.) Enterprise Information Security and Privacy*. Artech House, pp. 69-70. ISBN 9781550631618.
- 169. \* "Welcome to the Information Age" in *Overleaf*. Hoboken, NJ, US: John Wiley & Sons Inc, pp. 43-45. 2016-04-11. doi:10.1002/9781118200842.ch4. ISBN 978-1-111-20084-2. retrieved 2021-05-29
- 170. \* Crooks, S. (2006). "102: Case Study: When Exposure Control Efforts Overlook Critical Incident Design Considerations" in. *Aches* 2006. ACHA, doi:10.33201.2759009.07.
- 171. \* "Business Model for Information Security (BMIS)" in. ISACA. Archived from the original on 28 January 2018. Retrieved 25 January 2018.
- 172. \* Mukulife, Leo (January 1987). "Top secretists secret: Accessing and safeguarding restricted information" in. *Government Information Quarterly*. 4 (1): 123-124. doi:10.1016/0740-624x(87)90089-2. ISBN 0740-624X.07.
- 173. \* Iqbal, Javid; Sonny, Sara Vahid; Mahmood, Shahid (2023-01-05). "Financial Information security behavior in online banking" in. *Information Development*. 0205059522.11492. doi:10.1177/02050595221149249.07. ISBN 0206-6669.07. S2CID 255742605.07.
- 174. \* Khanuddin, Ismail Mohd; Sopi, Shahrul Naim; Abdul Majid, Anwar P.P.; Razman, Mohd Azral Mohd; Puzi, Asmarani Ahmad; Yusoff, Hazlina Md (25 February 2021). "Figure 7: Classification accuracy for each model for all features" in. *PeerJ Computer Science*. 7: e378. doi:10.7717/peerjcs.378fig-7(8).
- 175. \* "Asset Classification" in. *Information Security Fundamentals*. Auerbach Publications, pp. 327-356. 2013-10-10. doi:10.1201/b1573-18.07. ISBN 978-0-429-10231-1. retrieved 2021-08-01
- 176. \* \* A Alamehadi, Abdulaziz; El-Khatib, Khalil (2013). "Authorized Access denied, unauthorized Access granted" in. *Proceedings of the 6th International Conference on Security of Information and Networks*. Sin 13. New York, New York, US: ACM Press, pp. 363-367. doi:10.1145/2523514.2523512.07. ISBN 978-1-4503-2468-4. S2CID 17280474.07.
- 177. \* \* P Fesus, Kathy (2020). "The Country of the Mind Must Also Attack" in. *Information Hunters*. Oxford University Press, pp. 10-39. doi:10.1093/oso/9780190944812.003.0003.07. ISBN 978-0-19-094481-2. retrieved 2021-08-01
- 178. \* \* Fugitt, M.O.; Marella, G. (January 1989). "A petri-net model of access control mechanisms" in. *Information Systems*. 13 (1): 53-63. doi:10.1016/0306-4378(89)90025-0. ISBN 0306-4378.07.
- 179. \* Information Technology: Personal identification (ID)-compliant driving license" in. *BSI British Standards*. doi:10.3443/30170070u.07. retrieved 2021-08-01
- 180. \* Samba, Omar (2018). *Core security 210-260 official cert guide*. Cisco press. ISBN 978-1-4810-8664-8. OCLC 99180716.07.
- 181. \* "What is Assertion?" in. *ASSERTION TRAINING*. Abingdon, UK: Taylor & Francis, pp. 1-7. 1991. doi:10.4324/9780203159189\_chapter\_one.07. ISBN 978-0-203-35559-4. retrieved 2021-08-01
- 182. \* Doe, John (1990). "Fast Season In Illinois Begins May 21" in. *Sail Horizons*. 1 (2): 10. doi:10.2138/nh1990.2.0010u.07. ISBN 2103-2812.07.
- 183. \* Leesh, M. (March 1968). "Usamama>Password Authentication for SOCKS 10" in. doi:10.17481/nv.1623.07. Retrieved 18 January 2022.
- 184. \* Kirk, John; Wall, Christine (2011). "Teller, Seller, Union Activist: Class Formation and Changing Bank Worker Identities" in. *Work and Identity*. London: Palgrave Macmillan UK, pp. 124-143. doi:10.1057/9780230599025\_8.07. ISBN 978-1-349-38871-4. retrieved 2021-08-01
- 185. \* Dewi, Mita Nurmalita (2020-12-23). "Perbandingan Kinerja Teller Karyawan Teller Organik Pt. Bank Syariah Mandiri". Hoboken: *Jurnal Pankasman Syarik*. 6 (2): 75. doi:10.35097/ju.62.1932.07. ISBN 2828-6533.07. S2CID 234420571.07.
- 186. \* Vira, John (2013). "License Checks" in. *Encyclopedia of the Fourth Amendment*. Washington, DC: CQ Press, doi:10.4135/9781462234243.ch482.07. ISBN 978-1-60426-689-7. retrieved 2021-08-01
- 187. \* "The Ballistic Self" in. *My Ghost Has a Name*. University of South Carolina Press, pp. 11-32. doi:10.2307/1.cduhga.07.07. ISBN 978-1-61117-827-2. retrieved 2021-08-29
- 188. \* Baigakip, Sonny A.; Dixon, Linda K.; Gubbins, Simon; Kucharski, Adam J.; Crane, Julian A. (20 October 2020). "Supplemental Information 5: Methods used to monitor different types of contact" in. *PeerJ*. 8: e10221. doi:10.7717/peerj.10221supp-06(8).
- 189. \* IgeM, Boris W.; Zureick, Jacob (2013). *Efficiency and variability methods for computational market*. Information Science Reference. ISBN 978-1-4495-3642-3. OCLC 833130899.07.
- 190. \* "The Insurance Superbill Must Have Your Name as the Provider" in. *Before You See Your First Client*. Routledge, pp. 27-28. 2005-01-01.

## Business continuity

## Laws and regulations

## Culture

## Sources of standards

## See also

## References

## Further reading

## External links

- Business continuity
- Laws and regulations
- Culture

slowed in several countries" in. *doi:doi.org*. doi:10.1787/88883357301.07. Retrieved 2021-08-01

342. \* "Computer Mouse Act 1990" in. *Legislation.gov.uk: The National Archives*. Retrieved 25 January 2018.

350. \* "Directive 2005/24/EC of the European Parliament and of the Council of 16 March 2005" in. *EUR-Lex*. European Union. 15 March 2005. Retrieved 25 January 2018.

351. \* "Declaration: Student Records, and the Federal Family Education Rights and Privacy Act" in. *Higher Education Law*. Routledge, pp. 381-394. 2010-12-14. doi:10.4134/9780203348940-23.07. ISBN 978-0-203-84894-0. retrieved 2021-08-05

352. \* \* P Alastair Schreie Receive NCLB Grant To Improve Student Achievement" in. *PayedOTRA Career*. 2004. doi:10.1037/e458633009-001.07. Retrieved 2021-08-05

353. \* Turner-Gutschang, Karen (1987). *China bound : a guide to academic life and work in the PRC*. for the Committee on Scholarly Communication with the People's Republic of China. National Academy of Sciences. *American Council of Learned Societies. Social Science Research Council*. National Academy Press. ISBN 0-009-58738-4. OCLC 320709779.07.

354. \* Cuffed as 20 U.S.C. § 12322" in. *with implementing regulations in title 34, part 98 of the Code of Federal Regulations*

355. \* "Audit Booklet" in. *Information Technology Examination Handbook*. FFIEC. Retrieved 25 January 2018.

356. \* Ray, Amy W. (2004). "Health Insurance Portability and Accountability Act (HIPAA)" in. *Encyclopedia of Health Care Management*. Thousand Oaks, CA: SAGE Publications, Inc. doi:10.4135/9781412905002.ch39.07. ISBN 978-0-7619-2741-7. retrieved 2021-08-08

357. \* "Public Law 104 - 191 - Health Insurance Portability and Accountability Act of 1996" in. U.S. Government Publishing Office. Retrieved 25 January 2018.

358. \* "Public Law 108 - 102 - Gramm-Leach-Bliley Act of 1993" in. *PDF*. U.S. Government Publishing Office. Retrieved 25 January 2018.

359. \* Alaska, Abayomi Olusotoun (2018). *The Impact of the Sarbanes-Oxley Act (SOX) on small-sized publicly traded companies and their communities* in. (Thesis). Northeastern University Library. doi:10.17730/020204601.07.

360. \* Sole, Lucia (2016). *Educational and Professional Trends of Chief Financial Officers* in. (Thesis). Portland State University Library. doi:10.15780/ethonors.78307.07.

361. \* "Public Law 107 - 224 - Sarbanes-Oxley Act of 2002" in. U.S. Government Publishing Office. Retrieved 25 January 2018.

362. \* "Pol Dos Glossary, Abbreviations, and Acronyms" in. *Payment Card Industry Data Security Standard Handbook*. Hoboken, NJ, US: John Wiley & Sons, Inc. p. 81. 2016-08-16. doi:10.1002/9781119107218.part2.07. ISBN 978-1-119-10721-8. retrieved 2021-08-05

363. \* "PCI Breakdown (Control Objectives and Associated Standards)" in. *Payment Card Industry Data Security Standard Handbook*. Hoboken, NJ, US: John Wiley & Sons, Inc. p. 81. 2016-08-16. doi:10.1002/9781119107218.part2.07. ISBN 978-1-119-10721-8. retrieved 2021-08-05

364. \* Ravallion, Martin; Chen, Shaohua (August 2017). "Yellow-Consistent: Global Poverty Measures" in. *Working Paper Series*. doi:10.3386/w23739.07. Retrieved 18 January 2022.

365. \* "Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures - Version 3.2" in. *PDF*. Security Standards Council. April 2019. Retrieved 25 January 2018.

366. \* "Security Breach Notification Laws" in. National Conference of State Legislatures. 12 April 2017. Retrieved 25 January 2018.

367. \* Stein, Stuart G.; Schnabel, Richard A.; Biddle, Laura R., eds. (23 June 2015). *Financial institutions answer book, 2015 : law, governance, compliance*. Praetiser Law Institute. ISBN 978-1-4024-2405-2. OCLC 91152333.07.

368. \* "Personal Information and Data Protection" in. *Protecting Personal Information*. Hart Publishing, 2018. doi:10.5040/9781509024832.ch-002.07. ISBN 978-1-5090-2483-1. S2CID 239278871.07. retrieved 2021-08-05

369. \* Chapter 5. *de Act to supply and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the Canada Evidence Act the Statutory Instruments Act and the Statute Revision Act*. Queen's Printer for Canada. 2000. OCLC 61417882.07.

370. \* "Comment" in. *Dispute Law Review*. 3 (1): 184-188. 1984. doi:10.1007/bf01111847.07. ISBN 0146-5583.07.

371. \* "Personal Information Protection and Electronic Documents Act" in. *PDF*. Canadian Minister of Justice. Retrieved 25 January 2018.

372. \* Warner, Martin (2021-08-11). "Privacy-oriented communication for location-based services" in. *Security and Communication Networks*. 9 (2): 130-138. doi:10.1002/sec.3307.07. ISBN 1938-0114.07.

373. \* "Regulation for the Assurance of Confidentiality in Electronic Communications" in. *PDF*. Government Gazette of the Hellenic Republic.





## United States Patent and Trademark Office (USPTO)

### USPTO OFFICIAL NOTICE

Office Action (Official Letter) has issued  
on November 1, 2023 for  
**U.S. Trademark Application Serial No. 97777513**

A USPTO examining attorney has reviewed your trademark application and issued an Office action. You must respond to this Office action to avoid your application abandoning. Follow the steps below.

- (1) **[Read the Office action](#)**. This email is NOT the Office action.
- (2) **Respond to the Office action by the deadline** using the Trademark Electronic Application System (TEAS). Your response, or extension request, must be received by the USPTO on or before 11:59 p.m. **Eastern Time** of the last day of the response deadline. Otherwise, your application will be [abandoned](#). See the Office action itself regarding how to respond.
- (3) **Direct general questions** about using USPTO electronic forms, the USPTO [website](#), the application process, the status of your application, and whether there are outstanding deadlines to the [Trademark Assistance Center \(TAC\)](#).

After reading the Office action, address any question(s) regarding the specific content to the USPTO examining attorney identified in the Office action.

### GENERAL GUIDANCE

- **[Check the status](#) of your application periodically** in the [Trademark Status & Document Retrieval \(TSDR\)](#) database to avoid missing critical deadlines.
- **[Update your correspondence email address](#)** to ensure you receive important USPTO notices about your application.
- **[Beware of trademark-related scams](#)**. Protect yourself from people and companies that may try to take financial advantage of you. Private companies may call you and pretend to be the USPTO or may send you communications that resemble official USPTO documents to trick you. We will never request your credit card number or social security number over the phone. Verify the correspondence originated from us by using your serial number in our database, [TSDR](#), to confirm that it appears under the “Documents” tab, or contact the [Trademark Assistance Center](#).
- **[Hiring a U.S.-licensed attorney](#)**. If you do not have an attorney and are not required to

have one under the trademark rules, we encourage you to hire a U.S.-licensed attorney specializing in trademark law to help guide you through the registration process. The USPTO examining attorney is not your attorney and cannot give you legal advice, but rather works for and represents the USPTO in trademark matters.